

Firewall Analyzer 7.2

Standalone/Collector Server - User Guide

www.fwanalyzer.com

Table of Contents

INTRODUCTION.....	5
About Firewall Analyzer	6
Release Notes	7
Supported Firewalls	9
INSTALLATION AND SETUP	12
System Requirements.....	12
Prerequisites.....	16
Installing and Uninstalling	18
Starting and Shutting Down	20
Accessing the Web Client.....	23
License Information	24
GETTING STARTED	25
Using the Dashboard	26
Using the Sub Tab	32
Using The Left Navigation Pane	34
Dashboard View Customization	36
Firewall Analyzer Reports	38
FIREWALL REPORTS	39
Live Reports	40
Application Reports.....	45
Traffic Reports	47
Protocol Usage Reports.....	49
Web Usage Reports	52
Mail Usage Reports	55
FTP Usage Reports	57
Telnet Usage Reports.....	60
Event Summary Reports.....	62
VPN Reports.....	64
Firewall Rules Report.....	68
Inbound Outbound Reports.....	70
Intranet Reports	72
Internet Reports	74

Streaming and Chat Sites Reports.....	76
Security Reports	78
Virus Reports.....	80
Attack Reports	83
Spam Reports.....	86
Admin Reports.....	88
URL Categories Reports.....	90
Firewall Change Management Reports.....	92
PROXY REPORTS	99
Live Reports	100
Top Talkers.....	105
Website Details.....	107
Proxy Usage	109
Proxy Server - URL Categories Reports	111
TREND REPORTS.....	113
Protocol Trend Reports.....	114
Traffic Trend Reports.....	115
Event Trend Reports.....	116
VPN Trend Reports	117
CUSTOM REPORTS	119
Creating Report Profiles.....	119
Setting Log Filters.....	122
Creating Custom Criteria Reports	124
Using Advanced Search	125
NOTIFICATIONS	128
Creating an Alert Profile.....	128
Viewing Alerts.....	136
Alerts Administration.....	137
SYSTEM SETTINGS.....	139
Simulating Firewall Logs	141
Configuring Data Storage Duration	142
Managing Syslog Servers	144
Managing LEA Servers.....	145
Managing Alert Profiles.....	147
Configuring DNS Resolution	149

Mapping User Name vs IP Address using DHCP/Proxy Logs	151
Importing Log Files	156
Viewing Device Details	160
Archiving Log Files	161
Configuring to Fetch Firewall Configuration and Unused Rules	164
Diagnose Firewall Connections.....	175
Scheduling Reports	177
Working Hour Configuration.....	179
Report View Customization.....	180
Rebranding Firewall Analyzer Web Client.....	181
ADMIN SETTINGS.....	183
Managing Protocol Groups	183
Setting up Intranets.....	186
Adding Different Users.....	187
Setting up the Mail Server.....	192
External Authentication Settings	193
RADIUS Server Configuration Settings.....	195
Setting up the Mail Server.....	197
Configuring Firewall Availability Alerts	198
Viewing Server Diagnostics	200
Accessing the Database	201
License Management - Manage/Unmanage Devices	202
SMS Settings.....	204
Changing Account Settings.....	206
CONFIGURING FIREWALLS.....	207
Configuring Check Point Firewalls	208
Configuring NetScreen Firewall	213
Configuring Cisco Devices - PIX/ASA/FWSM/VPN Concentrator.....	216
Configuring Microsoft ISA Server	227
Configuring CyberGuard	229
Configuring Cyberoam	230
Configuring Fortinet Firewalls	232
Configuring WatchGuard Firebox.....	236
Configuring Snort.....	238
Configuring Secure Computing Sidewinder.....	239

Configuring SonicWALL Internet Security Appliances	240
Configuring Juniper Devices	241
Configuring 3Com	245
X-Family Remote SysLog Configuration	245
Configuring IPCop Firewalls	250
CONFIGURE PROXY SERVER	251
Configuring Squid Proxy Server	252
TIPS AND TRICKS	254
Frequently Asked Questions	254
TROUBLESHOOTING TIPS	266
OTHER TOOLS AND UTILITIES	272
Configuring Firewall Analyzer Parameters	272
Configuring MSSQL Database	274
Moving Firewall Analyzer's database to different directory in the same server	278
Moving Firewall Analyzer Server installation to another server	281
Running Firewall Analyzer and MySQL database in different machines	283
Configuring Secure Communication - SSL	284
How to bind specific interface of the machine to Firewall Analyzer application?	289
How to move Firewall Analyzer Raw Logs Archive and Raw Logs Indexing directory to mapped network drive?	297
DISTRIBUTED EDITION - COLLECTOR SERVER	299
Installing and Uninstalling - Distributed Edition Collector Server	300
Troubleshooting Tips - Distributed Edition Collector Server	303
INTEGRATING FIREWALL ANALYZER WITH OPMANAGER	304
USING ASK ME	306
CONTACTING TECHNICAL SUPPORT	307

Introduction

A Firewall is an important perimeter defense tool which protects your network from attacks. Security tools like Firewalls, VPN's, and Proxy Servers generate a huge quantity of traffic logs, which can be mined to generate a wealth of security information reports.

What is Firewall Analyzer?

ManageEngine Firewall Analyzer is a browser-based firewall/VPN/proxy server reporting solution that uses a built-in syslog server to store, analyze, and report on these logs. Firewall Analyzer provides daily, weekly, monthly, and yearly reports on firewall traffic, security breaches, and more. This helps network administrators to proactively secure networks before security threats arise, avoid network abuses, manage bandwidth requirements, monitor web site visits, and ensure appropriate usage of networks by employees.

Firewall Analyzer analyzes your firewall and proxy server logs and answers questions like the following:

- Who are the top Web surfers in the company, and what web sites are they visiting?
- How many users inside the firewall are trying to access web sites with inappropriate content?
- How much network activity originates on each side of the firewall?
- Are we experiencing hack attempts? Where are they originating?
- Which servers receive the most hits?

This User Guide will help you install Firewall Analyzer on your machine, and get familiar with the Firewall Analyzer user interface. If you are unable to find the information you are looking for in this document, please let us know at fwanalyzer-support@manageengine.com

About Firewall Analyzer

Firewall Analyzer automatically collects, correlates, and analyzes security device information from enterprise-wide heterogeneous firewalls, and proxy servers from Cisco, Fortinet, CheckPoint, WatchGuard, NetScreen, and more.

The following are some of the key features of this release:

Feature	Description
Multiple firewall vendor support	Support for most leading enterprise firewall appliances, proxy servers, IDS, IPS and VPN security devices
Automated syslog collection and processing	Automatically collects and parses logs, and updates the database at user-defined intervals
Syslog archiving	Allows for archiving of log files at user-defined intervals. The archive files are encrypted, hashed and time stamped for tamper proof storage
Bundled database	Stores and processes syslog data in the bundled MySQL database. Allows you to use MS SQL database, if available in your enterprise.
Dashboard	Provides a quick view of current activity across all devices from a single place
Automatic alerting	Automatically notifies and warns against specific events based on user-defined thresholds. Reports on network behavioral analysis can be obtained from Anomaly Alert Reports.
Pre-defined device reports	Includes traffic analysis reports across all devices or specific to firewalls, and proxy servers
Historical trending	Allows you to analyze trends in bandwidth usage, protocol usage, etc. over varying time periods
Customizable report profiles	Allows you to build reports to meet your specific needs
Report scheduling	Automatically generates reports at specified time intervals and delivers them as PDF reports via email.
Multiple report formats	Generates and exports reports in HTML, PDF, and CSV formats.
Advanced user management	Allows you to create different users and set appropriate access privileges
Multi-platform support	Runs on Windows and Linux platforms

Release Notes

The new features, enhancements, and bug fixes in the 7.2.0 release are mentioned below.

- 7.2.0 - Build 7020 (GA)

7.2.0 - Build 7020

GA release of Firewall Analyzer

7.2.0 - Build 7020 - Distributed Edition

GA release of Firewall Analyzer Distributed Edition.

New Features - Collector Server

The general features available in this release include,

- Collector Server contains all the features of Firewall Analyzer Standalone Edition

7.2.0 - Build 7020 - Standalone Edition

The general features available in this release are:

New Features and Enhancements

1. New Device/Log Format supported
 - o Palo-Alto Firewall
 - o Juniper SSLVPN 6500
 - o Check Point VSX firewalls
 - o FortiGate Webfilter, DLP, IPS modules and IPSec support
2. Application reports for Fortigate firewalls based on Application Control service
3. Support for Virtual Firewalls of Cisco and Fortigate devices. By default, each context/vdom is displayed as separate device
4. Alerts based on bandwidth utilization of a specific interfaces
5. Client UI and email notification for Firewall Status Alerts for the following conditions:
 - o Lack of disk space
 - o Syslog server down
6. View unused ACEs details of ACLs, for Cisco devices available in Unused Rules report
7. Real-time Syslog collection from Squid proxy server supported
8. Complete time duration details of the VPN user sessions available in 'VPN User Session Details' reports under VPN Reports
9. Option to export 'VPN User Session Details' report to other formats, while clicking 'View All' link
10. Zone based and interface specific Live reports using SNMP for Netscreen devices
11. Change Management Report for Juniper SRX device available


12. Option to fetch Rules and Configurations for any CLI supported device to get Unused Rules, Compliance and Change Management reports
13. New format for Email alert to cater for context based Configuration Changes
14. Optional privilege available to 'Guest' user to view the generated alerts for the assigned device(s)
15. Optional privilege available to 'Guest' user to view the Report Profile(s) assigned by Administrators

Bug Fixes

1. Identifying Device IP address from the logs imported from Blue Coat proxy server
2. Collecting intermitant logs of VPN sessions support for Sonicwall, Cisco, Checkpoint and Netscreen Firewall devices
3. Added page navigation component in 'Raw Log Search' result page
4. Importing log files with non-English names/folders from remote machines using FTP is supported
5. Allowed special characters in SNMP Community string to fetch SNMP data from devices
6. Issue in Diagnose Connections when the interface name had special characters

Supported Firewalls

Firewall Analyzer is compatible with the following firewall devices.

	<ul style="list-style-type: none"> Information on configuring some of the following firewalls is available in the Configuring Firewalls section If the Firewall device logs contains the time zone information, Firewall Analyzer processes it and normalizes it to time zone of Firewall Analyzer Server
---	---

NetFlow Log Support

Cisco	Cisco ASA NetFlow Log
-------	-----------------------

Firewall Log Support

Company Name	Device/Version (versions up to)	WELF Certified	Other Log Format
3Com	3Com X-family Version 3.0.0.2090 or later. But earlier versions will work to a lesser extent.		✓
Anchiva	Secure Gateway Series 200, 500, 800, 1000, 2000		✓
Applied Identity	Identiforce		✓
ARKOON Network Security	ARKOON 2.20	✓	
Astaro	Astaro Security Linux v7.0, v8.0	✓	✓
Aventail	Extranet Center v3.0	✓	
AWStats	Most versions		✓
BlueCoat	SG Series		✓
CheckPoint	Log import from most versions, VSX Firewalls, LEA support for R54 and above		✓
Cimcor	CimTrak Web Security Edition	✓	
Cisco Systems	Cisco Pix Secure Firewall v 6.x, 7.x, Cisco ASA, Cisco IOS 3005, 1900, 2911, 3925, Cisco FWSM, Cisco VPN Concentrator, Cisco CSC-SSM Module 6.3.x, Cisco SSL WebVPN or SVC VPN, Cisco IronPort Proxy, Cisco Botnet module		✓
Clavister	Most versions		✓
CyberGuard	CyberGuard Firewall v4.1, 4.2, 4.3, 5.1	✓	
Cyberoam	Cyberoam Firewall Version: 9.5.4		✓
D-Link	Most DFL versions		✓
DP Firewalls	DP Firewall 1000-GE		✓
Electronic	IPTables Firewall		✓

Company Name	Device/Version (versions up to)	WELF Certified	Other Log Format
Consultants			
Fortinet	FortiGate family, Webfilter, DLP, IPS modules, and IPSec, SSL VPN - v300A, v310B	✓	✓
FreeBSD	Most versions		✓
Funkwerk UTM	Funkwerk Enterprise Communications		✓
Global Technologies	Gnatbox (GB-1000) 3.3.0+	✓	
IPCop	IPCop Firewall Version 1.4.17 / 1.4.18	✓	
Ingate	Ingate firewall: 1200, 1400, 1800/1880	✓	
Inktomi	Traffic Server, C—Class and E—Class	✓	
Juniper	6360, 8350 Series, SRX100, SRX210, SRX220, SRX240, SRX650, SRX1400, SRX3400, SRX3600, SRX5600, SRX5800, IDP, SSL VPN 4500 & 6500, New Format Logs NetScreen most versions of Web Filter & Spam Modules	✓	✓
Kerio	Winroute		✓
Lenovo Security Technologies	LeadSec		✓
Lucent	Security Management Server V. 6.0.471		✓
McAfee (formerly Secure Computing)	SnapGear, SG580, Sidewinder (uses SEF Sidewinder Export Format)	✓	✓
Microsoft	Microsoft ISA (Firewall, Web Proxy, Packet Filter, Server 2006 VPN) Server 2000 and 2004, W3C log format Threat Management Gateway (TMG)		✓
NetApp	NetCache		✓
NetASQ	F10, F100 v3.x	✓	
NetFilter	Linux Iptables		✓
Netopia	S9500 Security Appliance v1.6	✓	
Network-1	CyberwallPLUS-WS and CyberwallPLUS-SV	✓	
Palo Alto	Palo Alto Firewalls PA 5000 series		✓
Recourse Technologies	ManHunt v1.2, 1.21	✓	
Ruijie	Firewall		✓
Securepoint	Securepoint UTM Firewalls		✓
Snort	Most versions		✓
SonicWALL	SOHO3, SOHO TZW, TELE3 SP/TELE3 Spi, PRO 230, 2040, 3060, 4060, 5060, TZ 100/ TZ 100w, TZ 170, TZ 170 Wireless, TZ 170 SP Wireless, TZ 200/ TZ 200w, TZ 210/ TZ 210w, NSA 240, NSA 2400, NSA 2400MX, NSA 3500, NSA 4500, NSA 5000, NSA E5500, NSA E6500, NSA E7500, NSA E8500, NSA E8510	✓	✓
Squid Project	Squid Internet Object Cache v1.1, 2.x	✓	
St. Bernard Software	iPrism 3.2	✓	

Company Name	Device/Version (versions up to)	WELF Certified	Other Log Format
Sun Microsystems	SunScreen Firewall v3.1	✓	
WatchGuard	All Firebox Models v 5.x, 6.x, 7.x, 8.x, 10.x, 11, Firebox X series, x550e, x10e, x1000, x750e	✓	✓
Zywall	Most versions	✓	

Installation and Setup

System Requirements

This section lists the minimum system requirements for installing and working with Firewall Analyzer. Please refer our website for recommended system requirements.

- Hardware Requirements
- MySql Performance Improvement Parameters
- Supported Operating Systems
- Supported Web Browsers

Hardware Requirements

For 32 Bit Installation

The minimum hardware requirements for Firewall Analyzer to start running are listed below.

- 1 GHz, 32-bit (x86) Pentium Dual Core processor or equivalent
- 2 GB RAM
- 5 GB Hard disk space for the product

For 64 Bit Installation

The minimum hardware requirements for Firewall Analyzer to start running are listed below.

- 2.80 GHz, 64-bit (x64) Xeon® LV processor or equivalent
- 2 GB RAM
- 5 GB Hard disk space for the product

Firewall Analyzer is optimized for 1024x768 monitor resolution and above.

* The following table recommends the disk space and RAM size requirements of the system where Firewall Analyzer is installed. The disk space and RAM size requirements depends on the number of devices sending log information to Firewall Analyzer, the number of firewall log records received per second or the firewall log data received per day by Firewall Analyzer.

Recommended Minimum RAM Requirement

Log Records Rate	RAM Size
Up to 100 Logs/sec	1 GB
100 - 500 Logs/sec	2 GB
500 - 1000 Logs/sec	4 GB
Above 1000 Logs/sec	4 GB (64 Bit)
Above 1000 Logs/sec	8 GB

Hard Disk Space Requirement

The split up is: Archive+Index+MySQL=Total

Log Records Rate	For 1 Day	For 1 Week	For 1 Month
50 Logs/sec	$1+0.5+10.5=12$ GB	$5+3+30=38$ GB	$18+7+75=100$ GB
100 Logs/sec	$2+1+15=18$ GB	$10+5+50=65$ GB	$35+15+100=150$ GB
300 Logs/sec	$6+3+31=40$ GB	$30+15+105=150$ GB	$100+45+295=440$ GB
500 Logs/sec	$10+5+75=90$ GB	$50+25+225=300$ GB	$170+70+480=720$ GB
1000 Logs/sec	$20+10+150=180$ GB	$95+45+500=640$ GB	$325+125+950=1.4$ TB

Log Records Rate	For 3 Months	For 6 Months	For 1 Year
50 Logs/sec	$60+25+125=210$ GB	$120+40+160=320$ GB	$240+90+300=630$ GB
100 Logs/sec	$110+50+240=400$ GB	$220+80+320=720$ GB	$450+170+580=1.2$ TB
300 Logs/sec	$280+120+600=1$ TB	$500+200+800=1.5$ TB	$900+350+1250=2.5$ TB
500 Logs/sec	$470+230+1100=1.8$ TB	$900+400+2100=3.4$ TB	$1700+700+3600=6$ TB
1000 Logs/sec	$920+480+2100=3.5$ TB	$1750+750+4200=6$ TB	$2850+1250+6400=10.5$ TB

CPU Requirements

- Dedicated machine has to be allocated to process more than 200 logs per second.
- Dual core processors are needed to process more than 500 logs per second.
- Quadra core processors are needed to process more than 1000 logs second.

RAM Requirements

- Number of firewalls handled by the Firewall Analyzer will increase the requirement of the above RAM values. So it is better to have RAM value higher than the suggested value in case of having more than 5 firewalls.

Separate Installation

- Firewall Analyzer server and MySQL database can be installed in separate machines, in case of higher log rate with low-end CPU machines.

Hard Disk Requirements for more months

- The above Hard Disk space requirement projected is for one month. If you need to archive the logs for more number of months, multiply the above requirements with the number of months based on your requirement.

Note: The Log Records Per Second is the total log records received per second by Firewall Analyzer from all the configured devices.

MySQL Performance Improvement Parameters

For better performance, we recommend replacing the existing MySQL parameters mentioned in **startDB.bat/sh**, available under <FirewallAnalyzerHome>\bin directory, with the following MySQL parameters **changes** for the corresponding RAM Size.

RAM Size	MySQL Parameters For Windows Installation	MySQL Parameters For Linux Installation
512 MB	Default configuration as given in startDB.bat	Default configuration as given in startDB.bat
1 GB	--innodb_buffer_pool_size= 300M --key_buffer_size= 150M --max_heap_table_size= 150M --tmp_table_size= 100M --table-cache= 512	--innodb_buffer_pool_size= 300M --key_buffer_size= 150M --max_heap_table_size= 150M --tmp_table_size= 100M --table-cache= 512
2 GB	--innodb_buffer_pool_size= 900M --key_buffer_size= 600M --max_heap_table_size= 350M --tmp_table_size= 100M --table-cache= 512	--innodb_buffer_pool_size= 900M --key_buffer_size= 600M --max_heap_table_size= 350M --tmp_table_size= 100M --table-cache= 512
3 GB	--innodb_buffer_pool_size= 900M --key_buffer_size= 600M --max_heap_table_size= 350M --tmp_table_size= 100M --table-cache= 512	--innodb_buffer_pool_size= 1400M --key_buffer_size= 1000M --max_heap_table_size= 350M --tmp_table_size= 100M --table-cache= 512
4 GB	--innodb_buffer_pool_size= 900M --key_buffer_size= 600M --max_heap_table_size= 350M --tmp_table_size= 100M --table-cache= 512	--innodb_buffer_pool_size= 1800M --key_buffer_size= 1200M --max_heap_table_size= 350M --tmp_table_size= 100M --table-cache= 512

Supported Operating Systems

Firewall Analyzer has been tested to run on the following operating systems and versions:

- Windows™ 7/NT/2000/XP/Vista, 2000, 2003 and 2008 Server
- Linux - RedHat 8.0/9.0, Mandrake/Mandriva, SuSE, Fedora, CentOS

Note: If Firewall Analyzer is installed in SuSE Linux, then ensure that in the **mysql-ds.xml** file, present under <FirewallAnalyzer_Home>/server/default/deploy you replace *localhost* mentioned in the following line : <connection-url>jdbc:mysql://localhost:33336/firewall</connection-url> with the corresponding IP Address or DNS resolvable name of the current system where Firewall Analyzer is installed.

Supported Web Browsers

Firewall Analyzer has been tested to support the following browsers and versions:

- Internet Explorer 5.5 or later

- Netscape 7.0 or later
- Mozilla 1.5 or later
- Firefox 1.0 or later

Prerequisites

This topic deals with the following pre-requisites for setting up Firewall Analyzer in your enterprise.

- Ports to be Freed
- Recommended System Setup
- Changing Default Ports

Ports to be Freed

Firewall Analyzer requires the following ports to be free:

Port Number	Usage
8500	This is the default web server port. You will access the Firewall Analyzer server from a web browser using this port number. You may change this port during installation.
514, 1514	These are the default listener ports on which Firewall Analyzer listens for incoming logs exported from devices. You can add more ports on which Firewall Analyzer can listen for incoming logs.
33336	This is the port used to connect to the MySQL database in Firewall Analyzer



Look up Changing Default Ports for help on changing the default ports used by Firewall Analyzer

Recommended System Setup

Apart from the System Requirements, the following setup would ensure optimal performance from Firewall Analyzer:

- Run Firewall Analyzer on a separate, dedicated PC or server. The software is resource-intensive, and a busy processor may cause problems in collecting logs.
- Use the MySQL bundled with Firewall Analyzer that runs on port 33336. You need not start another separate instance of MySQL.

Changing Default Ports

Changing the default MySQL port:

1. Edit the **mysql-ds.xml** file present in the `<FirewallAnalyzer_Home>/server/default/deploy` directory.
2. Change the port number in the following line to the desired port number:
`<connection-url>jdbc:mysql://localhost:33336/firewall</connection-url>`
3. Save the file and restart the server.

Changing the default web server port:

1. Edit the **sample-bindings.xml** file present in the
 <FirewallAnalyzer_Home>/server/default/conf directory.
2. Change the port number in the following line to the desired port number:
 <binding port="8500"/>
3. Save the file and restart the server.

Installing and Uninstalling

Firewall Analyzer is available for Windows and Linux platforms. It is available both in 32 Bit version and 64 Bit version.

Installation Procedure for various OS and CPU versions:

- Windows 64 Bit version
- Windows 32 Bit version
- Linux 64 Bit version
- Linux 32 Bit version

For more information on supported versions and other specifications, look up System Requirements.

This topic covers the following procedures:

- Uninstalling Firewall Analyzer
- Windows
- Linux


Installing Firewall Analyzer

Windows 64 Bit version:

The Firewall Analyzer Windows 64 Bit version download is available as an EXE file at <http://manageengine.com/products/firewall/download.html>

Windows 32 Bit version:

The Firewall Analyzer Windows 32 Bit version download is available as an EXE file at <http://manageengine.com/products/firewall/download.html>

Rest of the installation procedure remains same for both 64 Bit and 32 Bit versions. Double-click the downloaded EXE file, and follow the instructions as they appear on screen. Once the installation is complete you will notice a  tray icon, which provides you with the following options.

Option	Description
Firewall Server Status	This option provides you details like <i>Server Name</i> , <i>Server IpAddress</i> , <i>Server Port</i> , <i>Server Status</i> .
Start WebClient	This option will open up your default browser and connect you to the web login UI of Firewall Analyzer Server, provided the server has already been started.
Shutdown Server	This option will shutdown the Firewall Analyzer Server.



The tray icon option is only available for Windows !

Linux:**Linux 64 Bit version:**

The Firewall Analyzer Linux 64 Bit version download is available as a BIN file at <http://manageengine.com/products/firewall/download.html>

Linux 32 Bit version:

The Firewall Analyzer Linux 32 Bit version download is available as a BIN file at <http://manageengine.com/products/firewall/download.html>

Rest of the installation procedure remains same for both 64 Bit and 32 Bit versions.

1. Download the BIN file, and assign **execute** permission using the command:
`chmod a+x <file_name>.bin`
 where *<file_name>* is the name of the downloaded BIN file.
2. Execute the following command: `./<file_name>.bin`



During installation if you get an error message stating that the temp folder does not have enough space, try executing this command with the `-is:tempdir <directory_name>` option, where *<directory_name>* is the absolute path of an existing directory. `./<file_name>.bin -is:tempdir <directory_name>`

3. Follow the instructions as they appear on the screen.

This will install Firewall Analyzer on the respective machine.

Uninstalling Firewall Analyzer**Windows:**

1. Navigate to the Program folder in which Firewall Analyzer has been installed. By default, this is **Start > Programs > ManageEngine Firewall Analyzer 7**
2. Select the option **Uninstall Firewall Analyzer**
3. You will be asked to confirm your choice, after which Firewall Analyzer is uninstalled.

Linux:

1. Navigate to the *<Firewall Analyzer Home>/server/_uninst* directory.
2. Execute the command `./uninstaller.bin`
3. You will be asked to confirm your choice, after which Firewall Analyzer is uninstalled.



At the end of uninstallation you will be taken to the Uninstallation Feedback Form where you can provide reasons for your product uninstallation. This would help us improve this product.

Starting and Shutting Down

Once you have successfully installed Firewall Analyzer, start the Firewall Analyzer server by following the steps below.

This topic covers the following procedures:

- Starting Firewall Analyzer
 - Windows
 - Linux
 - Start the service
- Shutting down Firewall Analyzer
 - Windows
 - Linux
 - Stop the service
- Configure Firewall Analyzer as Linux service

Starting Firewall Analyzer

Windows:

Click on **Start > Programs > ManageEngine Firewall Analyzer 7 > Firewall Analyzer** to start the server.

Alternatively, you can navigate to the *<Firewall Analyzer Home>\bin* folder and invoke the **run.bat** file.

Windows Service:

Ensure that the Firewall Analyzer application is installed as Windows Service. When you install with single click, by default it will be installed as Windows Services. If you have carried out custom installation, and chose not to install the application as Windows Service, carry out the procedure to convert the application installation as Windows Service. After this, carryout the following procedure to start as Windows Service.

- Go to the Windows **Control Panel**, Select **Administrative Tools > Services**.
- Right-click **ManageEngine Firewall Analyzer 7** and select **Start** in the menu.
- Alternatively, select **Properties**. The **<Service> Properties** screen opens up.
- In the **General** tab of the screen, check the **Service status** is "*Stopped*" and **Start** button is in enabled state and other buttons besides are grayed.
- Click **Start** button to start the server as windows service.

Linux:

Navigate to the *<Firewall Analyzer Home>/bin* directory and execute the **run.sh** file.

As soon as this is done, a command prompt window opens showing startup information on several modules of Firewall Analyzer. Once all the modules have been successfully created, the following message is displayed:

```
Server started.
Please connect your client at http://localhost:8500
```

where 8500 is replaced by the port you have specified as the web server port during installation.

Starting the Firewall Analyzer service in Linux

```
/etc/init.d/firewallanalyzer start
```

```
Check the status of Firewall Analyzer service
/etc/init.d/firewallanalyzer status
ManageEngine Firewall Analyzer 7.0 is running (15935).
```

Shutting Down Firewall Analyzer

Follow the steps below to shut down the Firewall Analyzer server. Please note that once the server is successfully shut down, the MySQL database connection is automatically closed, and all the ports used by Firewall Analyzer are freed.

Windows:

1. Navigate to the Program folder in which Firewall Analyzer has been installed. By default, this is **Start > Programs > ManageEngine Firewall Analyzer 6**.
2. Select the option **Shut Down Firewall Analyzer**.
3. Alternatively, you can navigate to the *<Firewall Analyzer Home>\bin* folder and invoke the **shutdown.bat** file.
4. You will be asked to confirm your choice, after which the Firewall Analyzer server is shut down.

Windows Service:

Ensure that the Firewall Analyzer application is installed as Windows Service. When you install with single click, by default it will be installed as Windows Services. If you have carried out custom installation, and chose not to install the application as Windows Service, carry out the procedure to convert the application installation as Windows Service. After this, carryout the following procedure to start as Windows Service.

- Go to the Windows **Control Panel**, Select **Administrative Tools > Services**.

- Right-click **ManageEngine Firewall Analyzer 7**, and select **Stop** in the menu.
- Alternatively, select **Properties**. The **<Service> Properties** screen opens up.
- In the **General** tab of the screen, check the **Service status** is "Started" and **Stop** button is in enabled state and other buttons besides are grayed.
- Click **Stop** button to stop the windows service.

Linux:

1. Navigate to the *<Firewall Analyzer Home>/bin* directory.
2. Execute the **shutdown.sh** file.
3. You will be asked to confirm your choice, after which the Firewall Analyzer server is shut down.

Stopping Firewall Analyzer service in Linux

```
/etc/init.d/firewallanalyzer stop
Stopping ManageEngine Firewall Analyzer 7.0...
Stopped ManageEngine Firewall Analyzer 7.0.
```

Check the status of the service again

```
/etc/init.d/firewallanalyzer status
ManageEngine Firewall Analyzer 7.0 is not running.
```

To configure Firewall Analyzer as service in Linux, after installation

Normally, the Firewall Analyzer is installed as a service. If you have installed as an application and not as a service, you can configure it as a service any time later. The procedure to configure as service, start and stop the service is given below.

To configure Firewall Analyzer as a service after installation, execute the following command.

```
sh configureAsService.sh -i
```

Usage of Firewall Analyzer service command

```
<Firewall Analyzer Home>/bin # /etc/init.d/firewallanalyzer
```

```
Usage: /etc/init.d/firewallanalyzer { console | start | stop | restart | status | dump }
```

Accessing the Web Client

Firewall Analyzer is essentially a firewall, VPN, and proxy server log analysis tool that collects, stores, and reports on logs from distributed firewalls, and proxy servers on the network.

Once the server has successfully started, follow the steps below to access Firewall Analyzer.

1. Open a supported web browser window
2. Type the URL address as ***http://<hostname>:8500*** (where *<hostname>* is the name of the machine on which Firewall Analyzer is running, and *8500* is the default web server port)
3. Log in to Firewall Analyzer using the default username/password combination of **admin/admin**.

Firewall Analyzer provides two more external authentication apart from the local authentication. They are **Active Directory** authentication and **Remote Authentication Dial-in User Service (RADIUS)** authentication. If you import users from Active Directory or if you add a RADIUS server details, you will find the **Options >>** link besides the **Login** button in the Firewall Analyzer Client UI Login screen. If you click the **Options >>** link, **Log on to** field will appear below the **Password** field. The Log on to field will list the following options:

- **Local Authentication** - If the user details are available in local Firewall Analyzer server user database
- **Radius Authentication** - If the user details are available in RADIUS server and dummy user entry should be available in local Firewall Analyzer server user database
- **Domain Name(s)** - If the details of the user of a domain is imported from Active Directory into the local Firewall Analyzer server user database

Enter the **User Name** and **Password**. Select one of the three options in **Log on to** (**Local Authentication** or **Radius Authentication** or **Domain Name**). Click **Login** button to log in to Firewall Analyzer Client UI.

Once you log in, you can start collecting firewall logs, generate reports, and more.



If you want to access the web client from the same machine on which Firewall Analyzer is installed, execute the **startClient.bat/.sh** file from the *<Firewall Analyzer Home>/bin* directory.



- On a Windows machine, you can also access the web client from the Start menu by clicking on **Start > Programs > ManageEngine Firewall Analyzer 7 > Firewall Analyzer Web Client**.
- On a Windows machine, you can also access the web client from the System Tray by right-clicking on **Firewall Analyzer Tray Icon > Start Web Client**.

License Information

After you log in to Firewall Analyzer, click the **Upgrade License** link present in the top-right corner of the screen. The License window that opens, shows you the license information for the current Firewall Analyzer installation.

The License window displays the following information:

- Type of license applied - Trial or Registered (Professional, Premium)
- Product version number
- Number of days remaining for the license to expire
- Maximum number of devices that you are allowed to manage

Upgrading your License


Before upgrading the current license, make sure you have the new license file from Zoho Corp. saved on that system.

1. Browse for the new license file, and select it.
2. Click **Upgrade** to apply the new license file.

The new license is applied with immediate effect.

Contact fwanalyzer-support@manageengine.com or sales@manageengine.com for any license-related queries.

If you want to monitor Firewall device in High Availability mode, ensure that Firewall Analyzer is bound to one source (that is a single IP Address/host name), then that source is considered as one device license.

	Note: Each Virtual Firewall (vdom) monitored separately will be considered as one Firewall device for license purpose. If the Virtual Firewall is combinedly monitored with physical device as one Firewall device source and not as separate Virtual Firewall, then the physical device source will be considered as one Firewall device for license purpose. You can configure this option in the product.
---	---

Getting Started

Once Firewall Analyzer has been successfully set up and started in your network, the next thing you need to do is start sending logs to the Firewall Analyzer server.

As soon as you log in, you will see the Dashboard. If no devices are sending logs to Firewall Analyzer, you will see a welcome screen, with options to help you get started.

The options are:

- [Configure Your Firewall](#)
- [Add Syslog Server](#)
- [Import Log File](#)
- [Simulate](#)

Each of those options is explained below:

Configure Your Firewall

If your firewall is capable of exporting logs to the displayed ports in Firewall Analyzer, then set the appropriate parameters in the firewall to do so. Click the **How do I do this?** link for specific instructions on setting up log exports on certain firewalls.

Add Syslog Server

If your firewall cannot export logs to the displayed ports in Firewall Analyzer, but can export logs to another port, click the **Add Syslog Server** link to add a virtual syslog server and start receiving exported logs on the newly configured port.

Import Log File

If your firewall cannot export logs, or you need to generate reports from a squid proxy server click the **Import Log File** link to import a log file from the local machine or a remote machine via FTP.

Simulate

If you do not want to receive log files from any device, but still generate reports, click the **Simulate** link to generate reports from sample firewall logs. You can later turn this off by clicking the **Stop Simulate** link from the **Settings** tab.

Using the Dashboard

The Dashboard is shown when the **Home** tab is clicked. It is the first page you see when you log in. You can also customize your **Dashboard Views** as per requirements.



Dashboard Views selection is available only in the **Home** tab.

Once the server has started receiving records, the Dashboard dynamically changes to display the current statistics for each device whose log files are analyzed. The Firewall Analyzer dashboard shows the:


- Traffic Overview Graphs
- Security Overview Graphs
- Traffic Statistics
- Security Statistics
- Basic Search
- Advanced Search

The **Traffic Overview** graphs shows protocol-wise distribution of traffic across each device. At one glance, you can see the total traffic generated by each protocol group across each device. You can also drill down from the bars in the graph to see specific protocol usage in the Protocol Usage Report.

The **Security Overview** graphs shows distribution of security events like attack, virus, port scans, etc.. generated across each device. Drill down from the bars in the graph to see the corresponding events generated.



Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting a port scan. Currently Firewall Analyzer recognizes the attribute denoting a port scan for Fortigate, NetScreen & CheckPoint firewall's alone.


The **Traffic Statistics** table, shows the Traffic Overview graph's data in more detail, with specific percentage values of incoming and outgoing traffic per protocol group across each device. The **Show** bar lets you view the the top 5(default) / 10 / 15 or All protocol groups, captured in the logs across the configured devices. You can click on the Traffic IN, Traffic OUT, and Total Traffic for each protocol group of the configured device to obtain the drill-downs of the traffic. If the  icon is displayed above the table, it indicates that intranet's have not been configured. You need to configure intranet's if you want to separate inbound and outbound firewall traffic.



Click the **Live Syslog** link is provided in **Home > Traffic Statistics > Device Name** (besides the Firewall device). This will show the live syslogs information for the specific firewall. This will give the live syslog details i.e., Source IP, Destination IP, Port and syslog informations, provided the interfaces (i.e., eth0 etc.) should be open. In Linux the application should be started using root user. You can apply filter on Source IP and Port to get live syslogs received from particular IP/Port. If you click **Live Syslog** link, the **Firewall Analyzer - Syslog Viewer** screen pops up. In the screen, on top you will find 'Receiving Syslog Packets. _ packets received' message appears. Below that there is a **Capture Filter** : option with **Host IP Address** and **Port**. This capture filter will help

you to watch the live syslogs from the filtered host and port. In the case, since you clicked from a specific device, the specific Firewall device information is loaded in to it by default. The fields of the syslog packets displayed are: **Source**, **Destination**, **Port**, and **Message**.

Click the **View Syslog** link is provided in **Home > Traffic Statistics > Device Name** (besides the Proxy device). Ensure that the device has data for the selected calendar time range. This will show the raw syslogs information for the specific proxy device. The traffic values in the table let you drill down to see traffic details for the corresponding protocol group in the Protocol Usage Report.


The  **Quick Reports** link provides you 'quick' access to the top level details of traffic like Top Hosts, Top Destinations, Top Conversations, Top Protocol Groups, Top Firewall Rules, Top VPN Reports, and Top Attack Reports for the corresponding firewall.

	Quick Reports for Squid Proxies will provide only the following reports: Top Hosts, Top Destinations, and Top Conversations.
---	--

The  icon next to the Unassigned protocol group indicates traffic details for protocols that have not been assigned to any protocol group. Click the icon, and under the **View Identifiers** tab, you can see the traffic details for each of these unassigned protocols. The **Assign Group** tab provides you with options to either associate these unknown protocols to the predefined Protocol Groups (and Protocols) or create a new Protocol Group (and Protocol). You can do this by selecting from the listed identifier and assigning it to either the pre-defined Protocol Group (and Protocol) or create a  new protocol group (and new Protocol).

Multiple Selection enables you to assign multiple identifiers to a particular protocol group (and protocol). **Single selection** enables you to assign each of the individual identifier to a particular protocol group (and protocol).

The **Security Statistics** table, shows the Security Overview graph's data in more detail, along with the distribution of the **Configured Alerts**.

Click the **View Syslogs** link is provided in **Home > Security Statistics > Device Name** (besides the Firewall device). Ensure that the device has data for the selected calendar time range. This will show the recent security events for the specific firewall. If you click **View Syslogs** link, the **Recent Security Events** screen pops up. In that screen you can view latest Security Events received from device for the time duration **<Last 15 Mins, Last 30 Mins, Last 1 Hour, Last 2 Hours, Last 3 Hours, Last 6 Hours>**. In the screen, on top you will find **Formatted Logs**, **Raw Logs** tabs. You can choose the tabs to view either formatted logs or raw logs. Click  **Configure Columns** to select the columns to be displayed for the formatted logs The columns are: *All Columns, Device, Host, User, Protocol, Destination, Date/Time, Virus/Attack, VPN, Severity, Rule Number/ID, Status, URL, Duration, Description, StartTime*. Below that, the number of lines of logs displayed are indicated in the **Showing : _ to _ of total _ logs** field. The number lines displayed per page is indicated in the **View per page : 5 [10] 20 25 50 75 100 250 500** field. Default value is 10. The default columns displayed are: *Host, Protocol, Destination, Date/Time, Status, Severity, and Description*. You can add or remove columns using **Configure Columns** icon given above.

The Configured Alerts are classified according to the priority as High, Medium, and Low. Clicking on the alert counts against *High, Medium, Low*, or *All Alerts* will list you

complete details like Alert Profile name, the generated time, the device for which the alert was raised, the alert priority, and the status of the alert.

The security statistics table provides you with the counts for **Attacks, Virus, Failed Logons, Security Events, Denied Events, Config Changes** and **Compliance Reports**.

Attacks: Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting an attack.

Virus: Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting a virus.



Currently Firewall Analyzer recognizes the attribute denoting a virus for almost all firewall's except Cisco Pix, whose log messages do not contain the attribute denoting a virus.

Failed Log Ons: Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting a failed log on.



Currently Firewall Analyzer recognizes the attribute denoting a failed log on for Fortigate, NetScreen, Cisco Pix, & Identiforce firewall's Failed Log Ons are not available for CheckPoint firewall's

Denied Events: Firewall Analyzer will recognize only those firewall log messages which contains the attribute denoting a denied request.

Security Events: The Security Events in Firewall Analyzer are based on the severity attributes *Emergency, Alert, Critical*, and *Error* only.





Since *Security Events* are based on severity attributes, they may also include the other events like *port scans, attacks, virus, failed log ons, security events*, and *denied events*.

Clicking on the counts against each of the above events in the security statistics table will lead you to the corresponding the quick reports for those events.


Compliance Reports: The Compliance Reports related to Firewall Rules/Policies Configuration/Changes. Clicking the report opens up with the rules related events.

Editing Device Details

Click the  (for firewall) or  (for squid) icon next to a device name to change the device's details. You can change the device's display name, up link speed and down link speed. The device name and the vendor type cannot be changed.



Up Link Speed and Down Link Speed determines the % IN Traffic and % OUT traffic.

Click the  icon to delete the device from the database. You are asked to confirm your choice, after which the device is permanently deleted.



When a device is deleted, all existing data pertaining to that device is permanently

	deleted from the database. Later if logs are received from that device, the device is added as a new device, and reports are generated. To stop this from happening, you need to configure the device to stop sending logs to Firewall Analyzer.
--	--

Search

Doing a search in Firewall Analyzer UI is easy. Firewall Analyzer offers both a Basic Search and Advanced Search in all the pages of the product. The search results can be saved as report profiles and can also be scheduled to run the search and mail the report profile on an hourly, daily, weekly, monthly or once only basis. But the reports profiles created via search **cannot be edited** and **will not contain graphical representation of data, and drill down facility**.

 **Basic Search**, enables you to search for the following :

Search for	Description
Hosts	Refers to the IP Address or DNS Names which were recorded in the firewall logs <i>example: 192.168.0.1, web-server</i>
Protocol Identifiers	Refers to the list of protocols and protocol identifiers that are available in the Protocol Groups page (Settings >> Protocol Groups) <i>example: 6969/tcp, icmp, IPSec</i>
User Names	Refers to the authenticated user name required by some firewall's <i>example: john, kate</i>
Attack	Refers to the attack name. <i>examples: UDP Snort, Ip spoof</i>
Virus	Refers to the Virus name. <i>examples: JS/Exception, W32/Mitglieder</i>

Advanced Search, offers numerous options for making your searches more precise and getting more useful results Aggregated Logs Database. It allows you to search from the Raw Firewall Logs.

In Advance Search, you can search the logs for the selected devices, from the aggregated logs database or raw firewall logs, and define matching criteria.

Selected Devices

In this section, you can choose the devices for which you want the logs to be searched. If no device is selected or you want to change the list of selected devices, select the devices.

1. Click **Change Selection** link.
2. **Select Devices from the list** window pops-up. In that window, All Devices with selection check box and individual devices with selection check boxes options are available.
3. Select the devices by selecting the check boxes as per your requirement. Click **OK** to select the devices and close the window or click **Cancel** to cancel the operation and close the window.

The selected devices are displayed in this section.

Search From

In this section, you can select one from the two options:

1. Aggregated Logs Database
2. Raw Firewall Logs
3. Raw Proxy Logs

1. Aggregated Logs Database

Select this option if you want to search from the aggregated logs database.

2. Raw Firewall Logs

Select this option if you want to search from the raw firewall logs. Selecting this option will enable the following options:

- a. **Raw VPN Logs**
- b. **Raw Virus/Attack Logs**
- c. **Raw Device Management Logs**
- d. **Raw Denied Logs**

Select the above logs options as per your requirement.

3. Raw Proxy Logs

Select this option if you want to search from the raw Proxy server logs. All Squid, ISA proxy logs will be indexed in real time (i.e., whenever imported).

Hence, all logs are searchable.

Define Criteria

This section, enables you to search the database for attributes using more than one following criteria's:

Criteria	Description
Protocol	Refers to the list of protocols and protocol identifiers that are available in the Protocol Groups page (Settings >> Protocol Groups) <i>example: 8554/tcp, rtsp, IPSec</i>
Source	Refers to the source host name or IP address (CIDR format also) from which requests originated
Destination	Refers to the destination host name or IP address (CIDR format also) to which requests were sent
User	Refers to the authenticated user name required by some firewall's <i>example: john, kate</i>
Virus	Refers to the Virus name. <i>examples: JS/Exception, W32/Mitglieder</i>
Attack	Refers to the attack name. <i>examples: UDP Snort, Ip spoof</i>
URL	Refers to the URL, which you want to search
Rule	Refers to the Firewall Rule, which you want to search
Device	Refers to the device from which logs are collected
Message	Refers to the log message texts stored in the DB

- If the search string exists then the search result will be intelligently displayed based on the report category in which it occurred.
- By default, the search is carried out for the time period selected in the Global Calendar present in the left pane of the UI.
- You can also search within the search results.

Advanced Search of Imported Firewall Logs

You can carry out Advanced Search on the imported Firewall logs.

Using the Sub Tab

The sub tab provides links to frequently accessed reports and tasks in Firewall Analyzer. It also shows the current server status using intuitive icons.





The following reports can be generated by clicking the corresponding links in the sub tab:



Link	Action
Interface/Zone Reports	View live traffic reports for the past one day for each firewall, on a 5-minute average. The Live Reports are available for each interface or zone of the device separately.
Application	View application reports for the selected firewall. You can select the device using the drop down list.

The following tasks can be done by clicking the corresponding links in the sub tab:

Link	Action
Add New	Alert Profile
	Report Profile
	Syslog Server
Import Logs	Import a log file from your local machine or through FTP
Advanced Search	Offers numerous options for making your searches more precise and getting more useful results. Reports can be scheduled from the search results.

The purpose of each icon in the sub-tab is described below:






Icon	Description
	Packet Count - the number of packets received from each device sending log files to the server. For troubleshooting, admin users can view the cumulative flow rate of logs received by Firewall Analyzer at the syslog listening ports from all the configured firewalls.
	Listening Ports - the list of ports at which the server is listening for logs and devices that are sending logs to the syslog server at the particular port. If any of the ports is down, then you would receive a message in web UI  "Syslog listener port is down"
	Live Syslog Viewer - View raw packets. This will give the live syslog details i.e., Source IP, Destination IP, Port and syslog informations, provided the interfaces (i.e., eth0 etc.) should be open. In Linux the application should be started using root user. You can apply filter on Source IP and Port to get live syslogs received from particular IP/Port. If you click Live Syslog Viewer icon, the Firewall Analyzer - Syslog Viewer screen pops up. In the screen, on top you will find

Icon	Description
	<p>'Receiving Syslog Packets. _ packets received' message appears. Below that there is a Capture Filter : option with Host IP Address and Port. This capture filter will help you to watch the live syslogs from the filtered host and port. In the case, since you clicked from a specific device, the specific Firewall device information is loaded in to it by default. The fields of the syslog packets displayed are: Source, Destination, Port, and Message.</p> <p>Note: If you click Live Syslog Viewer and you get the following error message 'Unable to open interfaces for listening syslogs', then carryout the steps given below: If the installation is on Linux OS, assign SuperUser permission to fetch the Syslog packets. If the installation is on Windows OS, execute the PacketCapture.bat file present in the <Firewall Analyzer Home>/bin directory and restart Firewall Analyzer to view the live packets.</p>
	<p>Unknown Packet details - No Unparsed Records. No unknown packets or unsupported log formats have been received by the server</p>
	<p>Unknown Packet details - The unparsed records are displayed in the table. Unknown packets have been sent to the server. Details such as, Device Name, SysLog server, SysLog Port, Record Format, Notification, and Delete are displayed.</p> <p>There is also a note 'Click here to check your Firewall configuration.'</p>

Using The Left Navigation Pane

The left navigation pane provides quick links to different tasks and reports in Firewall Analyzer. The components present in the left navigation pane depend on the tab that is currently selected.

The following is a list of all components found in the left navigation pane:

Component	Description
Dashboard Views	List all the custom dashboard views created by the user. 'All Devices' view is the default dashboard view.
Global Calendar	Allows you to select the time period for all reports from one place. By default, the current day's data from 00:00 Hrs to the current time is shown.
Firewalls	Includes links to generate reports for each firewall from which logs have been collected. Click on the  icon to customize the reports view for each of the listed firewall's Click on the  icon against each firewall to generate reports for that firewall alone in a new window. Click on the  icon against each firewall to obtain Quick Reports of the top level details of traffic like Top Hosts, Top Destinations, Top Conversations, etc for the corresponding firewall.
Squid Proxy Reports	Includes links to generate reports for each squid proxy server from which logs have been collected. Click on the  icon against each squid proxy server to generate reports for that squid proxy server alone in a new window. Click on the  icon against each squid proxy server to obtain Quick Reports of the top level details of traffic like Top Hosts, Top Destinations, and Top Conversations for the corresponding Squid Proxy.
Reports Across Devices	Includes links to generate reports across all devices from which logs have been collected
My Report Profiles	Includes links to generate custom reports created using the Add Report Profile link.
All Alerts	Includes links to view all the alert profiles created by the user, using the Add Alert Profile link.
My Alerts	Includes links to view all the alerts assigned to the operator user by admin or other operator user. Includes links to view all the alerts assigned to the admin user by himself or other operator user.
Bookmarks	Allows you to set a bookmark for the current page, and manage existing bookmarks

Most of the tasks in the left navigation pane can be done from the main tabs also, by clicking the corresponding links. The left navigation pane provides a quicker way to perform the same tasks.

Using Calendar

You can use the calendar to select a single date or range of days to view various details of the reports, alerts, and logs of the Firewalls.

There are two icons provided on top left corner of the calendar to select a single day or range of days. Refer the screen shot given below:



Dashboard View Customization

In the **Dashboard Views** section, you can see **Customize** link besides "*Dashboard Views:*" title to customize the dashboard view and a combo box listing all the available Dashboard Views with **All Devices** view on top.

To customize the dashboard view, click **Customize** link. **Dashboard View Customization** page appears. It lists all the dashboard views available to the user including **All Devices** view on top.

The dashboard view customization page lets users to:

- Create multiple dashboard views based on the devices assigned to the user. Each view can be configured to show a list of assigned devices. The created dashboard views are listed in the Dashboard Views combo box in the left hand side top of the Home tab.
- Edit any of the listed views, except the **All Devices** dashboard view.
- Set any one of the views as default dashboard view.
- Delete any of the listed views, except the **All Devices** view and the default dashboard view, if any of the created dashboard view is set as a default dashboard view.


To create a new device view

Click **Create Device View** link. The **Create Device View** screen pops-up. In that screen,



- Enter a name for the view in the **View Name** text box.
- Select the devices from the **Available Devices** list, and move it to the **Dashboard View Devices** list.
- Select the **Set this view as Default Home** check box option to make this view as the default dashboard view upon user login.
- Click **Update** to create the device view and **Close** to close the screen.






Now you can see the new view created is listed in the **Dashboard View Customization** page.

To edit a device view

To edit a view, click the  icon of the view to be edited. The **Edit Device View** screen pops-up. The procedure is same as that of create device view.

To set a device view as default view

Select any one of the listed views to be **Set as default**. The default dashboard view is indicated by the  icon and all other views by the  icon.

Click the  icon of the view, which you want to set as default view. Now the  icon changes to  icon and in the previous default view, the  icon changes to  icon.

To delete a device view

To delete a view, click the  icon of the view to be deleted.




Default View: The default dashboard view is the one which appears in the **Home** tab, upon user login. By default **All Devices** view is set as default view. User can create and set any view as default view. Default view will appear automatically only when the user closes the client and re-logs in. User can view any of the listed dashboard views and traversing between the tabs will not change the view.

Firewall Analyzer Reports

Firewall Analyzer offers a rich set of pre-defined reports that help in analyzing bandwidth usage and understanding network behavior. On a broad level, reports in Firewall Analyzer are classified into the following types:

Report	Description
My Report Profiles	Create custom report profiles to report on specific parameters
Reports Across Devices	View bandwidth usage, protocol usage, etc. across all devices whose logs are analyzed
Firewall Reports	View traffic reports, protocol usage, event summary, etc. for each firewall
Squid Proxy Reports	View top talkers, site details, and squid usage summary for each squid proxy server
Trend Reports	View trends of bandwidth usage, protocol usage, and events generated

All the above reports can be accessed from the **Reports** tab. Except the **Live Report**, all other reports include links to several sections of the report which can be seen when the  icon, or the report bar itself is clicked. Click on each section to go to the corresponding section of the report directly, or click the **View Report** link to view the entire report with all the sections.

DNS Resolution in Reports


Firewall Analyzer provides an option to configure DNS resolution for all the reports. For more details refer Configuring DNS Resolution page under the **System Settings** section. In each of the individual reports a **ResolveDNS** link has been provided at the top. Clicking this link enables DNS Resolution for all the IP Addresses of the unresolved hosts present in the current report. The status of DNS Resolution depends on the default DNS lookup time, within which Firewall Analyzer will try to resolve the IP Address. If DNS Resolution is in progress for any other Firewall Analyzer user, then the subsequent user will see the message "*Please wait, DNS Resolution in progress for another user*" when clicking ResolveDNS link. Once the DNS Resolution is complete for the first user, then the DNS Resolution for the subsequent user begins automatically.

Firewall Reports

Firewall Analyzer offers a rich set of pre-defined reports that help in analyzing bandwidth usage and understanding network behavior.

The following reports are generated based on Firewall logs:

- Live Reports
- Traffic Reports
- Protocol Usage Reports
- Web Usage Reports
- Mail Usage Reports
- FTP Usage Reports
- Telnet Usage Reports
- Streaming & Chat Reports
- Event Summary Reports
- VPN Reports
- Firewall Rules Reports
- Inbound & Outbound Traffic
- Intranet Reports
- Internet Reports
- Security Reports
- Virus Reports
- Attack Reports
- Spam Reports
- Protocol Trend Reports
- Traffic Trend Reports
- Event Trend Reports
- Admin Reports
- VPN Trend Report
- URL Categories Report
- Firewall Change Management Report

The **Firewall Reports** section in Firewall Analyzer includes reports that are based on Firewall logs. This section can be accessed from the left navigation pane or the **Reports** tab. All the reports include links to several sections of the report which can be seen when the  icon, or the report bar itself is clicked. Click on each section to go to the corresponding section of the report directly, or click the **View Report** link to view the entire report with all the sections.

The **Live Report** lists reports for a device, over specific time periods.

The **Application Report** lists reports for applications of a device, over specific time periods.

Live Reports

The **Live Reports** provide a live visual representation of the traffic load across network links. Graphs are similar to that of MRTG, with the aim of providing a simple way to see exactly how much inbound and outbound traffic was generated for each device.

- Interface/Zone Reports For all devices
- Live Reports of Each Firewall Device
- Live Reports of Each Squid Device



SNMP base Live report graphs are not available for virtual Firewalls (vdom).

Interface/Zone Reports (Live Reports For all devices)

Click the **Interface/Zone Reports** link in the sub tab to see the Interface wise live reports for all devices, for the last 24 hours, over a 5-minute average.

Interface/Zone Live Reports Dashboard (Last 24 Hours) screen opens up. In that screen you will find **Device - Interface details** table. It will list all the devices and their interfaces. Click the **Show All** link or **+ tree** icon to the left of the device in the list. **Hide All** link or **- tree** icon will display the list of devices and the numbers of interface the device has. The expanded table lists the **Device Name**, **Interface Name**, **Bandwidth IN**, and **Bandwidth OUT**. Bandwidth IN and Bandwidth Out will display the bandwidth usage of the interface in percentage and the average speed in Kbps.

Click on the **Live Reports** link below the device in the list to view the live reports for that device alone.

Click on the individual interfaces names of the device in the list to view the only the live reports of the interface of the device.

Configure SNMP protocol settings for your Firewall device

The procedure to configure the SNMP protocol settings of Firewall devices in the Firewall Analyzer is given below:

- Click **Interface/Zone Reports > Click Configure SNMP protocol for Live reports. "Try now."** link. **Add Live Settings** page appears.
- In that, the devices are listed in the **Device Name** drop down list. Select the device as required.
- Below the **Device Name**, the **IP Address** of the selected device will appear.
- Select the **SNMP Version V1** or **V2** or **V3** using the respective radio button.
 - **Version 1 (V1):**
 - Enter the **SNMP Community** of the device in the text box
 - Enter the **SNMP Port** of the device in the text box
 - **Version 2 (V2):**
 - Enter the **SNMP Community** of the device in the text box
 - Enter the **SNMP Port** of the device in the text box
 - **Version 3 (V3):**

- Enter the **SNMP Community** of the device in the text box
- Enter the **SNMP Port** of the device in the text box
- Enter the **User Name** of the device in the text box
- Enter the **Context Name** of the device in the text box
- **Authentication:**
 - Select the **Protocol** for authentication from the drop down list (**MD5, SHA**).
 - Enter the **Password** for authentication in the text box
- **Encryption:**
 - Select the **Protocol** for encryption from the drop down list (**DES, AES**).
 - Enter the **Password** for encryption in the text box
- Select the reports in the **Select Reports** section. In that section, the **Report Name** and **Protocol** are listed.
- Select **Interface Live Report** using the check box. Select the **Protocol** for the report. On selecting the **Interface Live Report**, **Interval** field will appear with the drop down list. You can select **1 minute** or **5 minutes** or **10 minutes** granularity in Live reports by choosing appropriate interval.
- Select **Live VPN Users** report using the check box. Select the **Protocol** for the report. This report will be listed only if the device has the provision to get the Live VPN Users using SNMP protocol. Otherwise, this report option will not be there.
- The **Apply to other similar devices** section, contains list of devices of the same vendor type as the selected device with the check boxes to select, along with **Select All** devices option. If you want to apply the same credentials (Community, Port, etc..) to other similar firewalls, please select them.
- Click **Save** button to save the configuration and **Cancel** button to cancel the operation. Upon saving the form, the details are stored in the database and a sample SNMP query is made to test connection. If the SNMP credentials are not valid, you can skip saving the **Live Settings**.




If SNMP query is not successful, error message will be displayed on top of the page. Upon error, ensure the credentials provided are correct. Also ensure you have provided Management access through the source interface for SNMP protocol.


Once the '**Live Settings**' is added successfully, the **Edit | Disable | Delete SNMP** options are displayed to respective devices in **Interface Live Reports** Dashboard. The Live Reports and Interface Live Reports are populated with SNMP data.

Using the SNMP parameters configured, all the devices will be queried to get interface details. To configure/enable SNMP protocol in individual Firewall devices, refer the respective device configuration documents. Fortigate, Netscreen, Cisco PIX, Cisco ASA, Cisco Firewalls using ASDM tool

Once the SNMP settings is done for Live Reports, we skip the syslog data and use SNMP data for Live Reports. To switch to syslog option either disabling or deleting the SNMP settings. You could find this option to the right of device name in Interface/Zone Live Reports dashboard.

Configuring SNMP parameters for specific interfaces

Before the interface name, you will find  icon. Click the icon to set the **Interface Details** specific to this interface. **Configure Interface Details** screen pops-up. On the top you will see two options, one is **User Input** and the other is **Get from SNMP query** with radio buttons.

By default **User Input** radio button is selected. If you want to manually enter the interface details, carryout in this screen as given below: In the **User Input** screen, **Device Name**, **Interface Name** will be displayed. Besides the name of the interface, you will find  edit icon. Click the icon to change the interface name as per your requirement. The result will take effect immediately. You can enter the **Interface IP**, **Interface IP**, **Up Link Speed (in Kbps)**, and **Down Link Speed (in Kbps)** values manually.

Select the **Get from SNMP query** radio button if you want the application to automatically query the interface through SNMP and fetch the interface details. In the **Get from SNMP query** screen, **Device Name** will be displayed and you can enter the **Device IP Address**, **SNMP Community** and **SNMP Port**. Enter the the **SNMP Community** and **SNMP Port** parameters. Using the SNMP parameters configured, the specific interface will be queried to get interface details.

Click **Save** button to save the configuration and **Cancel** button to cancel the operation.



SNMP base Live report graphs are populated based on SNMP OID's ifInOctets and ifOutOctets. As these OID's are incremental counters we do not plot graph at a point when any of these counters gets reset.

Live Reports of Each Firewall Device

On the top right side of the Report screen, there will be two combo boxes. They are:

- Refresh
- Export as

Refresh

The **Refresh** combo box lets to enable or disable refreshing of the Live reports and lets you to choose the refreshing interval of the Live reports. There will be three field values for filtering. They are:

- Never Refresh
- Refresh Every 1 Min
- Refresh Every 5 Min
- Refresh Every 10 Min

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).


Click the **Live Reports** link present inside the list of reports for a device, to see the live reports for that device alone, over all the time periods described above.

The graphs for each device shows the minimum, maximum, and average amount of incoming and outgoing traffic through that device, over several time periods. Traffic is broken down into the last day, last week, last month, and last year, with an average granularity of 5 minutes, 30 minutes, 2 hours, and 1 day respectively.

The incoming and outgoing bandwidth can be viewed in Kbps.

Drill down from each of the graphs in the live report to see the following details:

Graph	Description
Inbound/Outbound Traffic Conversations	The inbound/outbound conversations for all hosts across this device. This data is available only for the last day's traffic over a 5-minute average granularity.
Top Hosts	The top hosts contributing to inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations for each host, during the selected time period.
Top Protocol Groups	The top protocol groups used in inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations using each protocol group, during the selected time period.
Top Users	The top users contributing to inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations for each user, during the selected time period.

	Live Reports will not be available for devices whose logs do not contain the "duration" field. For example: <i>WatchGuard, SonicWall, Astaro, IP Filter Linux Firewall, etc...</i>
---	---

Live Reports of Each Squid Proxy Device

On the top right side of the Report screen, there will be two combo boxes. They are:

- Refresh
- Export as

Refresh

The **Refresh** combo box lets to enable or disable refreshing of the Live reports and lets you to choose the refreshing interval of the Live reports. There will be three field values for filtering. They are:

- Never Refresh
- Refresh Every 1 Min
- Refresh Every 5 Min
- Refresh Every 10 Min

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Click the **Live Reports** link present inside the list of reports for a device, to see the live reports for that device alone, over specific time periods.

The graphs for each device shows the minimum, maximum, and average amount of outgoing traffic through that device, over several time periods. Traffic is broken down into the last day, last week, last month, and last year, with an average granularity of 5 minutes, 30 minutes, 2 hours, and 1 day respectively.


The outgoing bandwidth can be viewed in Kbps.



Live Reports will not be available for devices whose logs do not contain the "duration" field.

Application Reports

The **Application Reports** are available only for **Fortigate** Firewalls. This section includes reports that help in monitoring the bandwidth consumed by the application accessed by user like Skype, Facebook, Youtube etc.

	<p>Note:</p> <ul style="list-style-type: none"> • Ensure that the Fortigate Firewall has Application Control service to generate Application logs, which is for creating Application reports. • The Application report is available only in Standalone and Collector servers of Firewall Analyzer
---	--

Select the device using **Select Device:** <> drop down list to get the Application reports

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Schedule Report

You can schedule the report to be generated at pre-configured periodic interval.

On demand Application report can be created.

The **Application** graph shows distribution of application events like Skype, Facebook, Youtube, etc. generated for each selected device. At one glance, you can see the total traffic generated by each application/category across each device. You can also drill down the pie-chart to see specific application usage.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this application
Top Protocols	The top protocols used in this application
Top Users	The top users generating traffic using this application
Top Conversations	The top conversations carried out by this application

The **Top Hosts** graph shows the top hosts contributing to application traffic to the firewall. The table below the graph shows the host name or IP address, along with the number of hits and the total bytes of traffic generated.

The **Top Protocols** graph shows the top protocols contributing to application traffic to the firewall. The table below the graph shows the protocol, along with the number of hits and the total bytes of traffic generated.

The **Top Users** graph shows the top users contributing to application traffic to the firewall. The table below the graph shows the users, along with the number of hits and the total bytes of traffic generated.

The **Top Conversations** table lists details like host which initiated the conversation, its destination, the protocol used for the conversation, the application category along with the number of hits, the total bytes of traffic generated and % of total traffic for the particular conversation.

The table, shows the graph's data in more detail, with specific percentage values of incoming and outgoing traffic per application/category for the selected device. The **Show** bar lets you view the the top 5(default) / 10 / 15 or All application groups, captured in the logs. You can click on the Traffic IN, Traffic OUT, Total Traffic for each application of the configured device to obtain the drill-downs of the traffic.

The table lists details like host which initiated the conversation, its destination, the protocol used for the conversation, the user along with the number of hits and the total bytes of traffic generated for the particular application traffic.

Columns	Description
Applications	The list of applications accessed using the selected Firewall
Categories	The list of application categories accessed using the selected Firewall
Traffic In (MB)	The % of total traffic and amount of inward traffic that was generated by the application/category
Traffic Out (MB)	The % of total traffic and amount of outward traffic that was generated by the application/category
Total Traffic (MB)	The % of total traffic and amount of total traffic that was generated by the application/category

Traffic Reports

The **Traffic Reports** section includes reports that show bandwidth usage based on the amount of traffic sent and received through the device.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received**

graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocol Groups	The top protocol groups used by these hosts
Top Destinations	The top destination hosts or IP addresses accessed by these hosts
Rules Triggered	Firewall rules that were triggered by these hosts

The **Top Protocol Groups - Sent** and **Top Protocol Groups - Received** graphs show the top protocol groups sending and receiving data across the device respectively. The **Top Protocol Groups - Sent + Received** graph shows the top protocol groups grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the protocol group name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top protocols in this protocol group
Top Hosts	The top hosts generating traffic using protocols in this protocol group
Top Users	The top users generating traffic using protocols in this protocol group
Top Destinations	The top destinations accessed by protocols in this protocol group
Top Conversations	The overall top conversations through this protocol group

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users (Sent + Received)** graph shows the top users grouped by summing the number of bytes sent and received by each. The table below each graph shows the user name, number of hits, and the number of bytes sent or received or both as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocol Groups	The top Protocol Groups through which higher volume of data transferred.
Top Destinations	The top destinations accessed by user to transfer data
Top Hosts	The top hosts used by user, that transferred higher volume of data.
Rules Triggered	The Rules (policy violation, etc) that were triggered by the user while transferring data..

The **Events Generated** pie-chart shows the number of events generated, grouped by event severity. The table below the graph shows the event severity, number of events generated with that event severity, and the number of bytes of traffic generated.

Drill down from the pie-chart to see the following details:

Graph	Description
Top Hosts	The top hosts that generated events of this severity

Protocol Usage Reports

The **Protocol Usage Reports** section includes reports that show bandwidth usage based on all the protocol groups generating traffic through the device.



Separate reports are available for Web, Mail, FTP, and Telnet protocol groups. Click on the respective reports to view bandwidth usage details.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).



Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocol Groups - Sent** and **Top Protocol Groups - Received** graphs show the top protocol groups sending and receiving data across the device respectively. The **Top Protocol Groups - Sent + Received** graph shows the top protocol groups grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the protocol group name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top protocols in this protocol group
Top Hosts	The top hosts generating traffic using protocols in this protocol group
Top Users	The top users generating traffic using protocols in this protocol group
Top Destinations	The top destinations accessed by protocols in this protocol group
Top Conversations	The top conversations using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by each protocol group during working hours, which is the daily average value since the time the server was started.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by each protocol group during non-working hours, which is the daily average value since the time the server was started.

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Destinations	The top destination hosts or IP addresses accessed by these hosts
Top Users	The top users using this host in generating traffic
Traffic Distribution - Working Hours	The amount of traffic that was generated by the host during working hours, which is the daily average value since the time the server was started.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by the host after working hours, which is the daily average value since the time the server was started.

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received**

graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Destinations	The top destinations accessed by the user
Top Hosts	The top hosts used by user in generating traffic
Traffic Distribution - Working Hours	The amount of traffic that was generated by the user during working hours, which is the daily average value since the time the server was started.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by the user after working hours, which is the daily average value since the time the server was started.

The **Top Rules** table shows the top protocol groups triggering firewall rules, the (Rule Number IDs) rules that were triggered, the destination and the number of hits.

Web Usage Reports

The **Web Usage Reports** section includes reports on the top protocols under the Web protocol group, that have been used to generate traffic through that device.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).



Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocols - Sent** and **Top Protocols - Received** graphs show the top Web protocols sending and receiving data across the device respectively. The **Top Protocols - Sent + Received** graph shows the top protocols grouped by summing the number of bytes sent and received by each protocol. The table below each graph shows the protocol name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this protocol
Top Destinations	The top destinations accessed by using this protocol
Top Conversations	The top conversations using protocols in this protocol group

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Web protocols used by this user
Top Destinations	The top destination hosts or IP addresses accessed by this user using Web protocols
Top Hosts	The top hosts used by this user to generate traffic using Web protocols

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Web protocols used by this host
Top Destinations	The top destination hosts or IP addresses accessed by this host using Web protocols
Top Conversations	The top conversations initiated by host using protocols in this protocol group

The **Top URLs** table shows the top URL's or web sites that were accessed using protocols in the Web protocol group.

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the hosts triggering the rules.



Look up Managing Protocol Groups for help on adding, editing, and deleting protocol groups and protocols.

Mail Usage Reports

The **Mail Usage Reports** section includes reports on the top protocols under the Mail protocol group, that have been used to generate traffic through that device.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).



Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocols - Sent** and **Top Protocols - Received** graphs show the top Mail protocols sending and receiving data across the device respectively. The **Top Protocols - Sent + Received** graph shows the top protocols grouped by summing the number of bytes sent and received by each protocol. The table below each graph shows the protocol name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this protocol
Top Destinations	The top destinations accessed by using this protocol
Top Conversations	The top conversations using protocols in this protocol group

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Mail protocols used by this user
Top Destinations	The top destination hosts or IP addresses accessed by this user using Mail protocols
Top Hosts	The top hosts used by this user to generate traffic using Mail protocols

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Mail protocols used by this host
Top Destinations	The top destination hosts or IP addresses accessed by this host using Mail protocols
Top Conversations	The top conversations initiated by host using protocols in this protocol group

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the destination and the number of hits.



Look up Managing Protocol Groups for help on adding, editing, and deleting protocol groups and protocols.

FTP Usage Reports

The **FTP Usage Reports** section includes reports on the top protocols under the FTP protocol group, that have been used to generate traffic through that device.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).



Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocols - Sent** and **Top Protocols - Received** graphs show the top FTP protocols sending and receiving data across the device respectively. The **Top Protocols - Sent + Received** graph shows the top protocols grouped by summing the number of bytes sent and received by each protocol. The table below each graph shows the protocol name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this protocol
Top Destinations	The top destinations accessed by using this protocol
Top Conversations	The top conversations using protocols in this protocol group

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top FTP protocols used by this user
Top Destinations	The top destination hosts or IP addresses accessed by this user using FTP protocols
Top Hosts	The top hosts used by this user to generate traffic using FTP protocols

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top FTP protocols used by this host
Top Destinations	The top destination hosts or IP addresses accessed by this host using FTP protocols
Top Conversations	The top conversations initiated by host using protocols in this protocol group

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the destination and the number of hits.

The **Top URLs** table shows the top URL's or web sites that were accessed using protocols in the FTP protocol group.



Look up Managing Protocol Groups for help on adding, editing, and deleting protocol groups and protocols.

Telnet Usage Reports

The **Telnet Usage Reports** section includes reports on the top protocols under the Telnet protocol group, that have been used to generate traffic through that device.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).



Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocols - Sent** and **Top Protocols - Received** graphs show the top Telnet protocols sending and receiving data across the device respectively. The **Top Protocols - Sent + Received** graph shows the top protocols grouped by summing the number of bytes sent and received by each protocol. The table below each graph shows the protocol name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this protocol
Top Destinations	The top destinations accessed by using this protocol
Top Conversations	The top conversations using protocols in this protocol group

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Telnet protocols used by this user
Top Destinations	The top destination hosts or IP addresses accessed by this user using Telnet protocols
Top Hosts	The top hosts used by this user to generate traffic using Telnet protocols

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Telnet protocols used by this host
Top Destinations	The top destination hosts or IP addresses accessed by this host using Telnet protocols
Top Conversations	The top conversations initiated by hosts, using protocols in this protocol group

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the destination and the number of hits.



Look up Managing Protocol Groups for help on adding, editing, and deleting protocol groups and protocols.

Event Summary Reports

The **Event Summary Reports** section includes reports that show the summary of events generated by that device.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Hosts** graph shows the top hosts generating events along with the respective event severities. The table below the graph shows the host name or IP address, the event severity, the number of events, and the number of bytes of traffic generated.

Drill down from this graph to see the following graphs:

Graph	Description
Top Event Messages	The top event messages generated and corresponding event ID

The **Event Summary** pie-chart shows the number of events generated, grouped by event severity. The table below the graph shows the event severity, number of events generated with that event severity, and the number of bytes of traffic generated.

Drill down from the pie-chart to see the following details:

Graph	Description
Top Hosts	The top hosts that generated events of this severity
Top Event Messages	The top event messages received with this severity along with the hosts which generated them

Event Messages will list all the event messages in the descending order of number of events along with the severity.

VPN Reports

The **VPN Reports** shows usage statistics, protocols used, and other details across each VPN configured behind the firewall.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **VPN User Session Time Details** table shows the VPN session time details of each user. The table contains the user names of the Users, Start Time, End Time and Duration of the VPN sessions.

The **Top VPN Users** graph shows the top VPN users across all VPNs behind this firewall. The table below the graph shows each user, along with duration of the VPN connection, the number of hits, and the total bytes of traffic generated by each user.

Drill down from the graph to see the following details for each user:

Graph	Description
Top VPN Protocol Groups	List of Protocol Groups through which this User transferred higher volume of data.
Top VPN Hosts	List of VPN Hosts used by this User..
Top Destinations	List of Destinations Accessed by this User.
Top VPN Clients	List of VPN Clients used by this User.
Top Conversations	List of conversations started by this User.
VPN Summary	The bandwidth used by this User across each VPN
VPN Usage - Working Hour	VPN bandwidth used by this User during working hours, which is the daily average value since the time the server was started.
VPN Usage - Non-working Hours	VPN bandwidth used by this User after working hours, which is the daily average value since the time the server was started.

The **Top Failed VPN Users** graph shows the top VPN users with number of failed login attempts across all VPNs behind this firewall. The table below the graph shows each user, and the number of attempts.

Drill down from the graph to see the following details for each user:

Graph	Description
Hosts	List of VPN Hosts used by this User.
Reason	The reason for failed login attempt.
Hits	Number of failed login attempts.

The **Top VPN Hosts** graph shows the top hosts using bandwidth across all VPNs configured behind this firewall. The table below the graph shows the host names or IP addresses along with duration of the VPN connection, the number of hits, and the total bytes of traffic generated by each host.

Drill down from the graph to see the following details for each host:

Graph	Description
Top Protocol Groups	The top protocol groups used by this host. This graph drills down further to show the top users using these protocols.
VPN Summary	The bandwidth used by this host across each VPN
Top VPN Users	List of VPN users connecting through this host.
Top Destinations	The top Destinations Accessed by this host.
Top Clients	The top clients used by this host.
Top Conversations	The top conversations through this host.
VPN Usage - Working Hours	VPN bandwidth used by this host during working hours, which is the daily average value since the time the server was started.
VPN Usage - Non-working Hours	VPN bandwidth used by this host after working hours, which is the daily average value since the time the server was started.

The **Top VPN Clients** graph shows the top clients accessing the VPN. The table below the graph shows the host names or IP addresses along with the number of hits, and the total bytes of traffic transferred by each client.

Drill down from the graph to see the following details for each host:

Graph	Description
Top Protocol Groups	The top protocol groups Protocol Groups through which the client transferred higher volume of data.
Top VPN Users	The top VPN users connecting through the Client.
Top VPN Destinations	The top Destinations Accessed through Client.
Top Conversations	The top conversations connecting through Client.
VPN Summary	The list of VPNs used by Client
VPN Usage - Working Hours	VPN Usage during Working Hours by client, which is the daily average value since the time the server was started.
VPN Usage - Non-working Hours	VPN Usage during non Working Hours by client, which is the daily average value since the time the server was started.

The **Top VPN Protocol Groups** graph shows the top protocol groups used by VPNs behind this firewall. The table below the graph shows each protocol group, along with the number of hits, and the total bytes of traffic generated by each protocol group.

Drill down from the graph to see the following details for each protocol group:

Graph	Description
Top VPN Hosts	The top hosts behind the VPN using these protocol groups. This graph drills down further to show the top users using these protocols.
VPN Summary	The bandwidth used by this protocol group across each VPN
Top Destinations	List of Destinations Accessed through this protocol group.
Top Clients	List of Clients using this protocol group.
Top Conversations	List of VPN conversations through this protocol group.

The **VPN Usage Report** shows the total bandwidth used by each VPN behind this firewall. The table below shows the VPN gateway used, the number of hits, and the total bytes of traffic generated by each VPN.

Drill down from the graph to see the following details for each VPN:

Graph	Description
Top Protocol Groups	The top protocol groups used by this VPN. This graph drills down further to show the top hosts using these protocols.
Top VPN Hosts	The top hosts or IP addresses using this VPN
Top Destinations	The top Destinations Accessed through Client.
Top Clients	The top clients using the VPN
Top Conversations	The top conversations through VPN.
VPN Usage - Working Hour	Bandwidth used by this VPN during working hours, which is the daily average value since the time the server was started.
VPN Usage - Non-working Hour	Bandwidth used by this VPN after working hours, which is the daily average value since the time the server was started.

The **VPN Traffic Usage Trend** graph shows the hourly trend in VPN traffic across all VPNs configured behind this firewall. The table below the graph shows the the number of hits, and the total bytes of traffic received and sent for each hour of the day by all the VPNs.

Firewall Rules Report

The **Firewall Rules Report** shows the top firewall rules triggered on this firewall, grouped by different categories.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Used Rules** table shows the used Firewall rules and number of log counts that have triggered the firewall rules. The table shows the Rule Number or ID of the used

rule, and the Count of log entries that have triggered the particular rule. Drill down from the rule to see the hosts, protocols, user, status, message, total bytes consumed by the rules and count that triggered the firewall rule. The drilled down report also displays the total bytes consumed by the rules.

The **Top Unused Rules** table shows the Firewall rules that have not triggered. The table shows the Rule Number or ID of the unused rule. Drill down from the rule to see the description of the unused rule.

Top Unused ACEs

In the case of Cisco devices, the table shows the unused ACL and the exact unused ACEs. Drill down from the ACL to see the description of the unused ACEs.

The **Top Rules - Protocol Group Based** graph shows the top protocol groups that have triggered firewall rules. The table below the graph shows the protocol group, the rule triggered, and the number of hits. Drill down from this graph to see the top hosts, the top protocols and the top conversations that triggered the firewall rule in that protocol group.

The **Top Rules - Host Based** graph shows the top hosts that have triggered firewall rules. The table below the graph shows the host, the rule triggered, the number of hits. Drill down from this graph to see the top destinations accessed, the top protocols and the top conversations for each host that triggered the firewall rule.

The **Top Rules - Destination Based** graph shows the top destinations for which firewall rules have been triggered. The table below the graph shows the destination host name or IP address, the rule triggered, and the number of hits. Drill down from this graph to see the top hosts, the top protocols and the top conversations that triggered the firewall rule.

The **Top Rules** table shows the overall top firewall rules that have been triggered across this firewall. The table below the graph shows the rule triggered, and the number of hits. Drill down from this graph to see the top hosts, the top protocols and the top conversations that triggered the firewall rule.

Inbound Outbound Reports

The **Inbound Outbound Traffic Reports** section includes reports that show traffic details when inbound traffic (traffic coming into LAN) and outbound traffic (traffic going out of LAN) for the firewall, are separated. In order to separate inbound and outbound traffic, you need to first configure your intranets by clicking the **Intranet Settings** link from the **Settings** tab. When configured, the **Inbound Outbound Traffic Reports** shows you which hosts and what protocol groups have been contributing the most traffic on either side of the firewall.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary


Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:


- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Hosts - Inbound Firewall Traffic** graph shows the top hosts contributing to traffic inbound (traffic coming into LAN) to the firewall. The table below the graph shows the host name or IP address, along with the number of hits and the total bytes of traffic generated.

	If the host (IP / DNS Name of the machine which initiated the conversation) is INSIDE the LAN (Internal Host), then their RECEIVED will be counted as inbound and If the host (IP / DNS Name of the machine which initiated the conversation) is OUTSIDE the LAN (External Host) then their SENT will be counted as inbound.
---	--

The **Top Hosts - Outbound Firewall Traffic** graph shows the top hosts contributing to traffic outbound (traffic going out of LAN) to the firewall. The table below the graph shows the host name or IP address, along with the number of hits and the total bytes of traffic generated.

	If the host (IP / DNS Name of the machine which initiated the conversation) is INSIDE the LAN (Internal Host), then their SENT will be counted as outbound and If the host (IP / DNS Name of the machine which initiated the conversation) is OUTSIDE the LAN (External Host) then their RECEIVED will be counted as outbound.
---	--

The **Top Protocol Groups - Inbound Firewall Traffic** graph shows the top protocol groups contributing to traffic inbound to the firewall. The table below the graph shows the protocol group, along with the number of hits and the total bytes of traffic generated.

The **Top Protocol Groups - Outbound Firewall Traffic** graph shows the top protocol groups contributing to traffic outbound to the firewall. The table below the graph shows the protocol group, along with the number of hits and the total bytes of traffic generated.

Intranet Reports

The **Intranet Reports** section includes reports that show details of traffic transferred through the firewall by the internal hosts (hosts inside your LAN). In order to identify your internal hosts, you need to first configure your intranets by clicking the **Intranet Settings** link from the **Settings** tab.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Internal Hosts (Sent+Received)** graph shows the top internal hosts that are sending and receiving traffic through the firewall. You can expect only IP's **inside your LAN** here. The table below the graph shows the IP address, along with the number of hits, bytes received, bytes sent, and the total bytes (sent + received) of traffic generated.

The **Top Internal Protocol Groups (Sent+Received)** graph shows the top protocol groups used by internal host for sending and receiving traffic through the firewall. The table below the graph shows the protocol group, along with the number of hits, % hits, total bytes of traffic generated and what % of traffic each protocol group constitute to the total traffic.

The **Top Internal Servers** graph shows the top internal servers that served traffic. This is destination based report which list the internal servers which served more for external hosts. Transaction is not started/initiated by the servers listed here. Here you can expect all your server IPs which are behind your firewall, i.e. inside your LAN. The table below the graph shows the IP address of the internal server, along with the number of hits, the total bytes of traffic, and % of total traffic to the particular internal server.

The **Top Conversations** table lists details like host which initiated the conversation, its destination, the protocol used for the conversation along with the number of hits, the total bytes of traffic generated and % of total traffic for the particular conversation.

Internet Reports

The **Internet Reports** section includes reports that show details of traffic transferred through the firewall by the external hosts (hosts outside your LAN). In order to identify your external hosts, you need to first configure your intranets by clicking the **Intranet Settings** link from the **Settings** tab. When configured, all hosts outside your configured intranets will be considered as external hosts.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top External Hosts (Sent+Received)** graph shows the top external hosts that are sending and receiving traffic through the firewall. Here you can expect only IP's **outside your LAN**. The table below the graph shows the IP address, along with the number of hits, bytes received, bytes sent, and the total bytes (sent + received) of traffic generated.

The **Top External Protocol Groups (Sent+Received)** graph shows the top protocol groups used by external host for sending and receiving traffic through the firewall. The table below the graph shows the protocol group, along with the number of hits, % hits, total bytes of traffic generated and what % of traffic each protocol group constitute to the total traffic.

The **Top External Sites** graph shows the top external sites that were visited. This is destination based report which list the external servers or sites which served more for the internal hosts. Transaction is not started/initiated by the servers listed here. You can expect all external sites which are browsed more by your internal hosts. The table below the graph shows the host name or IP address, along with the number of hits, the total bytes of traffic to the site, and % of total traffic to the particular external site.

The **Top Conversations** table lists details like host which initiated the conversation, its destination, the protocol used for the conversation along with the number of hits, the total bytes of traffic generated and % of total traffic for the particular conversation.

Streaming and Chat Sites Reports

The **Streaming and Chat Sites Reports** section includes reports on streaming and chat sites visited. In order to identify your external hosts, you need to first configure your intranets by clicking the **Intranet Settings** link from the **Settings** tab. When configured, all hosts outside your configured intranets will be considered as external hosts.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Streaming and Chat Sites** graph shows the top streaming and chat sites that are sending and receiving traffic through the firewall. Here you can expect only IP's **outside your LAN**. The table below the graph shows the IP address, along with the number of hits, bytes received, bytes sent, and the total bytes (sent + received) of traffic generated.

The **Top Protocols** graph shows the top protocols used for accessing the streaming and chat sites through the firewall. The table below the graph shows the protocol used by the internal host to access the streaming and chat site, along with the absolute number of hits, bytes received, bytes sent, and the total bytes (sent + received) of traffic generated.

The **Top Sources** graph shows the top hosts that accessed the streaming and chat sites. The table below the graph shows the internal host accessing the streaming and chat site, along with the number of hits, bytes received, bytes sent, and the total bytes (sent + received) of traffic generated.

The **Top Attacks Using Streaming and Chat Protocols** table lists details like host, its destination, the protocol used for the conversation, the name or id (as defined by the firewall) of the attack, the attack count, status of the attack, and the attack message generated by the firewall.

Security Reports

The **Security Reports** section includes reports that help in monitoring and analyzing the security and effectiveness of the firewall, and assist in identifying, tracking, and investigating potential security risks.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Denied Hosts** report shows the top source IP addresses or host names that have been denied requests for the selected time period. The **Top Denied Destinations** report shows the top destination IP addresses or host names that have been denied responses for the selected time period.

Drill down from these graphs to see the following details:

Field	Description
Destination/ Host	The destination host name or IP address to which requests were denied/ The host name or IP address of the host whose requests were denied
Protocol	The protocol used by the denied request
Hits	The number of times the request was generated
Time	The timestamp of the last time when the request was received
Message	The message generated when the request was denied

The **Top Denied Protocols** report shows the top protocols that have been denied requests for the selected time period.

Drill down from this graph to see the following details:

Field	Description
Host	The host name or IP address of the host whose requests were denied
Destination	The destination host name or IP address that denied the request
Hits	The number of times the request was generated
Time	The timestamp of the last time when the request was received
Message	The message generated when the request was denied

The **Top Security Events** pie-graph shows the top events generated with severity as Emergency, Critical, Alert, Error, or Warning.

Drill down from this graph to see the following details:

Field	Description
Host	The host name or IP address of the host generating denied events
Severity	The event severity of the event generated
Hits	The number of times the event was generated
Time	The timestamp of the last time when the event was generated
Message	The event message generated

The **Top Blocked URLs** report shows the top URLs that were blocked for the selected time period.

In this report you will see the following details:

Field	Description
Host	The host name or IP address of the host whose requests were pointing to blocked URLs
Destination	The destination host name or IP address that denied the request
URL	The URL of the web site which was blocked
Hits	The number of times the request was generated

Virus Reports

The **Virus Reports** section includes reports that show details on viruses that have been identified by the firewall. These reports help in identifying the top viruses and worms that have affected the network, analyze the extent of damage, and also track the source of the attack.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Virus Sending Hosts** report shows the top source IP addresses or host names from which viruses have been sent, along with the protocol used to send the virus. The **Top Virus Affected Hosts** report shows the top destination IP addresses or host names that have been affected by viruses, along with the protocol that was used to receive the virus.

Drill down from these graphs to see the following details:

Field	Description
Virus	The name of the virus that was sent or received
Destination/ Host	The destination host or IP address to which the virus was sent/ The host or IP address that sent the virus
Severity	The severity level of the virus, as defined by the firewall
File	The name of the virus file that was sent or received
Hits	The number of times the virus was sent to or received by the same host
Subtype	The subtype of the virus, as defined by the firewall
Time	The timestamp when the virus was sent or received
Message	The virus message generated by the firewall

The **Top Protocols Used By Viruses** report shows the top protocols used by each virus. The **Top Viruses By Priority** report shows the top severities with which viruses have been sent.

Drill down from these graphs to see the following details:

Field	Description
Host	The host or IP address that sent the virus
Destination	The destination host or IP address to which the virus was sent
Severity/ Protocol	The severity level of the virus, as defined by the firewall/ The protocol used to send the virus
File	The name of the virus file that was sent or received
Hits	The number of times the virus was sent to or received by the same host
Subtype	The subtype of the virus, as defined by the firewall
Time	The timestamp when the virus was sent or received
Message	The virus message generated by the firewall

The **Top Virus Files** report shows the top virus files that have been sent. The **Top Virus with Status** report shows the status of the Top Virus. Drill down from these graphs to see the following details:

Field	Description
Virus	The name of the virus that sent this file
Host	The host or IP address that sent the virus file
Destination	The destination host or IP address to which the virus file was sent
Protocol	The protocol used by the virus to send this virus file
Severity	The severity level of the virus, as defined by the firewall
Hits	The number of times the virus file was sent to the same host

Field	Description
Subtype	The subtype of the virus, as defined by the firewall
Time	The timestamp when the virus file was sent
Message	The virus message generated by the firewall

The **Top Virus Generator** report shows the source of generation for each virus and their distinct targets.

Drill down from these graphs to see the following details:

Field	Description
Host	The host or IP address that generates the virus
Distinct targets	The destination system or machine to which the virus was distinctly targetted at.

Attack Reports

The **Attack Reports** section includes reports that show details of attacks that have been identified by the firewall. These reports help in identifying the top attackers, the top targets for the attacks and other details like protocol used, the priority of the attack and the status of the attack.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Attackers** report shows the top source IP addresses or host names from which attacks are originating, along with the protocol used for the attack and the number of hits. The **Top Targets** report shows the top destination IP addresses or host names that have been attacked, along with the protocol used for the attack and the number of hits.

Drill down from these graphs to see the following details:

Field	Description
Attack	The name or id (as defined by the firewall) of the attack that was sent or received
Destination/ Host	The destination host or IP address to which the attack was sent/ The host or IP address that sent the attack
Severity	The severity level of the attack, as defined by the firewall
Hits	The number of times the attack was sent to or received by the same host
Subtype	The subtype of the attack, as defined by the firewall
Time	The time stamp when the attack was sent or received
Status	The status of the attack that was sent or received
Message	The attack message generated by the firewall

The **Top Protocols Used By Attacks** report shows the top protocols used by each attack. The **Top Attacks By Priority** report shows the top attacks classified based on priority like Alert, Emergency etc.

Drill down from these graphs to see the following details:

Field	Description
Host	The host or IP address that sent the attack
Destination	The destination host or IP address to which the attack was sent
Severity/ Protocol	The severity level of the attack, as defined by the firewall/ The protocol used to send the attack
Hits	The number of times the attack was sent to or received by the same host
Subtype	The subtype of the attack, as defined by the firewall
Time	The time stamp when the attack was sent or received
Status	The status of the attack that was sent or received
Message	The attack message generated by the firewall

The **Top Attacks with Status** report shows the status of the Top Attacks (ID or names) based on the number of hits. Drill down from this graph to see the following details:

Field	Description
Attack	The name or id (as defined by the firewall) of the attack that was sent or received
Host	The host or IP address that sent the attack file
Destination	The destination host or IP address to which the attack file was sent
Protocol	The protocol used by the attack to send this attack file
Severity	The severity level of the attack, as defined by the firewall

Field	Description
Hits	The number of times the attack file was sent to the same host
Subtype	The subtype of the attack, as defined by the firewall
Time	The time stamp when the attack file was sent
Status	The status of the attack that was sent or received
Message	The attack message generated by the firewall

The **Top Attacker by unique targets** report shows peer to peer attack details. The report lists the hosts from which attacks are originating along with number of unique/distinct destinations (hosts) targeted. Drill down from this graph to see the following details:

Field	Description
Destination	The destination host or IP address to which the attack file was sent
Attack	The name or id (as defined by the firewall) of the attack that was sent or received
Protocol	The protocol used by the attack to send this attack file
Status	The status of the attack that was sent or received
Count	No. of times the attack file was sent to the destination.
Message	The attack message generated by the firewall

Spam Reports

The **Spam Reports** section includes reports that show details on spams that have been detected by the firewall. These reports help in identifying the top spams that have affected the network, analyze the extent of damage, and also track the source of the spam attack.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Spam Generator** report shows the source of generation for each spam with sender Email address and the number of times the spam was sent. In this report you will see the following details:

Field	Description
Host	The host or IP address that generates the Spam
Sender	Sender Email address
Hits	Number of spam mail sent

Drilling down the graph or table will give destination of Email, recipient Email address.

The **Top Spam Receivers** report shows the top destination IP addresses or host names that have been receiving Spam, along with the recipient Email address and the number of times the spam was received. In this report you will see the following details:

Field	Description
Destination	The host or IP address that generates the Spam
Recipient	Recipient Email address
Hits	The number of times the Spam was sent by the same host

Drilling down the graph or table will give source of Email, sender Email address.

The **Top Spam Rules** table shows the overall top spam rules that have been triggered across this firewall. The table below the graph shows the rule triggered, and the number of hits.

In this report you will see the top spam rules got triggered and the number of times the rule got triggered.

Field	Description
Rule Number/ID	The Spam rule number/ID which was triggered
Hits	The number of times the Spam rule was triggered

Drilling down the table will give source and destination of Email, sender and recipient Email address.

Admin Reports

The **Admin Reports** is available only for **Cisco PIX, NetScreen, FortiGate, and Identiforce Gateway**. This section includes reports that help in monitoring and analyzing the firewall user access, and aid in meeting regulatory compliance requirements..

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown.

- Top 5
- Top 10
- Top 15
- Top 20
- Top 25

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Successful User Logon report shows the users who have successfully logged-in to the firewall along with the count. **Successful User Logoff** report shows the users who have successfully logged-out of the firewall along with the count.

Denied User Logons report shows the users who have unsuccessfully attempted logging in to the firewall along with the count.

Commands Executed report provides you with the details of the commands executed by the user in the Cisco PIX, FWSM, ASA, NetScreen, and Fortigate firewalls.

URL Categories Reports

The **URL Categories Reports** section includes reports on the categories of URL fetched from the Firewall logs. The logs contain the URL category information and the number hits on the URL categories. In the **URL Categories Report: <Firewall>**, the graph and the table lists the categories and the hits of **Top Allowed Categories** and **Top Denied Categories**. Click on the particular category of allowed or denied categories, to view the **Category Drill Down Report**. The **Category Drill Down Report** lists the **Top URLs**, **Top Sources** and **Top Destinations** of a particular category.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Category Drill Down Report** lists the **Top URLs**, **Top Sources** and **Top Destinations** of a particular category.

The **Top URLs accessed under <category> Category** table lists the URLs accessed under the particular category. The table shows the list of URLs accessed under the particular category and the number of hits.

Graph	Description
URLs	The list URLs accessed under the particular category
Hits	The number of hits for each URL under the particular category

The **Top Sources for <category> Category** table lists the URLs accessed under the particular category. The table shows the list of hosts from where the URLs were accessed under the particular category and the number of hits.

Graph	Description
Hosts	The list of hosts from where the URLs were accessed under the particular category
Hits	The number of hits for each URL under the particular category

The **Top Destinations for <category> Category** table lists the URLs accessed under the particular category. The table shows the list of destination in which the URLs were accessed under the particular category and the number of hits.

Graph	Description
Destinations	The list of destination in which the URLs were accessed under the particular category
Hits	The number of hits for each URL under the particular category

Firewall Change Management Reports

The **Firewall Change Management Reports** are available for all Firewall devices. Firewall Change Management Report keeps track of all the changes done to a Firewall configuration from the time the device is configured to be monitored by the Firewall Analyzer. It fetches Firewall device configuration using **Telnet** or **SSH** protocols.

This page describes the Firewall Change Management reports, alerts and the procedure to configure the device.

- Show Changes
- Startup-Running Conflict Report
- Change Management Email Alert
- Description of Startup and Running configuration
- How to configure the Firewall device to get change management reports
- Report Filter links

Security Administrator can keep track of the Firewall configuration changes with the periodic reports and real time alerts. Firewall Analyzer provides complete trail of configuration changes since the time it started to manage the changes in the Firewall device.

Show Changes

Click the **Dashboard > Security Overview graph > Config Changes events > Show Changes** link to get the difference between any two configuration versions. The screen displays critical information about who made the changes, at what time and on which file. The changes in configurations like Modified, Added and Deleted are highlighted in Blue, Green and Red colors respectively. Have a look at the snap shot of Configuration Difference screen below.

Configuration Diff...

Device Name : FO-ELD-ASA
Config File Type : running
Version No : 1
Changed by : admin
Created On : 2011-04-26 12:02:49.0

Config File Type : running
Version No : 8
Changed by : admin
Created On : 2011-04-26 18:04:07.0

Get Specific Diff

Show : All Diff Lines View Diff Lines : Previous Next Modified Added Deleted

237
243
245
249 snmp-server host inside 192.168.117.117
340 username mahiiii password lHuGuu8aPYHOBQle encrypted privilege 2

237 snmp-server host inside 192.168.111.23
243 snmp-server host inside 192.168.111.88
245 snmp-server host inside 192.168.111.99
249
340

☒ Sync Scroll

Startup-Running Conflict Report

The changes between current versions of the Startup and running configuration files are displayed in this report. In this report also who, what, when and which questions are answered and the changes are marked in color. Select **<Firewall> device reports > Change Management Reports > Startup-Running Conflict Report** link to get the conflict report. Look at the screen shot of conflict report.

Configuration Diff...

Device Name : FO-ELD-ASA
Config File Type : startup
Version No : 1
Changed by : admin
Created On : 2011-04-26 12:02:49.0

Config File Type : running
Version No : 8
Changed by : admin
Created On : 2011-04-26 18:04:07.0

Get Specific Diff

Show : All Diff Lines View Diff Lines : Previous Next Modified Added Deleted

1 show startup-config
3 : Written by enable_15 at 14:55:47.486 IST Thu Apr 21 2011
68 pager lines 24
237
243
245
249 snmp-server host inside 192.168.117.117
340 username mahiiii password lHuGuu8aPYHOBQle encrypted privilege 2
362

1 show running-config
3 :
68 no pager
237 snmp-server host inside 192.168.111.23
243 snmp-server host inside 192.168.111.88
245 snmp-server host inside 192.168.111.99
249
340
362 : end

☒ Sync Scroll

Change Management Email Alert

You can get a real time alert via Email or SMS when a configuration change is made. This will reduce your reaction time drastically to rectify any erroneous configuration. Have a look at the Email message.

ManageEngine Firewall Analyzer - Firewall Configuration Change Alert

Device Name - FO-ELD-ASA

Config File Type : running
Changed By : admin
Changed On : 2011-04-26 17:59:30.1

Deleted Contents:

snmp-server host inside 192.168.111.88

Context based Change Management Email Alert

You can change the format of real time alert via Email or SMS when a configuration change is made. This can be configured in the Firewall Analyzer in the **userConfig.do** screen.

Firewall Analyzer User Input

Configuration Parameters	
Data Crunching Limit Value :	<input type="text"/> Save Reset
PDF Report Row Count :	10 Save Reset
Minimum Disk Space Setting :	5 Save Reset
Destination By Port :	<input type="radio"/> true <input checked="" type="radio"/> false Save
Context Based Config Change :	<input checked="" type="radio"/> true <input type="radio"/> false Save
Nipper Location :	<input type="text"/> Save Reset
Admin User Groups :	Admin Users,Employe Save Reset
Virtual Firewalls :	Select Your Firewall Name ▼ Save

Have a look at the Email message.

Do you want to stop sending email Notifications for Configuration changes [Click Here](#).

ManageEngine Firewall Analyzer - Firewall Configuration Change Alert

Device Name - pix501ed

Config File Type : startup
 Changed By : N/A
 Changed On : 2011-10-11 17:20:29.153

Configuration Changes		<input type="checkbox"/> Modified	<input type="checkbox"/> Added	<input type="checkbox"/> Deleted
Before Changes	Changes Done			
: Written by enable_15 at 15:49:40.262 IST Thu Sep 22 2011	: Written by enable_15 at 14:22:41.048 IST Tue Oct 11 2011			
enable password .g9gWhhhPjXJ6KZo encrypted	enable password PVSASRJovmamnVkD encrypted			
	access-list just_a_try permit udp any any eq www			
logging trap notifications	logging trap informational			
logging host inside 192.168.111.98 17/1514				
logging host inside 192.168.111.219 17/1514				
logging host inside 192.168.111.110 17/1514				

Description of Startup and Running configuration

The security appliance loads the configuration from a text file, called the startup configuration.

When you enter a command, the change is made only to the running configuration in memory. You must manually save the running configuration to the startup configuration for your changes to remain after a reboot.

In short, running configuration is temporary and startup configuration is permanent. Firewall Analyzer provides the following Change Management Reports:

- **Running Configuration Changes Report**
- **Startup Configuration Changes Report**
- **Current Startup-Running Conflict Report**

Running Configuration Changes Report


The report shows all the changes done to the running configuration for the given period of time along with when and who did the particular change.

Startup Configuration Changes Report

The report shows all the changes done to the startup configuration for the given period of time along with when and who did the particular change.

Current Startup-Running Conflict Report

The report will show the current conflicts between the startup and running configurations.

	<ul style="list-style-type: none"> The three configuration reports, Running Configuration Changes Report, Startup Configuration Changes Report, and Current Startup-Running Conflict Report are applicable only for Cisco devices. Only Running Configuration Changes Report is applicable for Netscreen and Fortigate devices. The calendar date setting will not be applicable for this report. As name suggests, this report will show only conflicts/differences between the current startup and current running configurations.
---	--

How to configure the Firewall device to get change management reports

- All the details/credentials required to connect to Firewall using Telnet/SSH should be given by the user in the Device Rule Info page. (**Settings > Device Rule > Add Device Info** link).
- Fill all the details/credentials required to connect to the firewall using Telnet/SSH
- Enable '**Generate Change Management Report**' option to get Firewall Change Management Report. If any Notifications or scheduled reports are needed fill the details accordingly in the provided fields.

☒ Generate Change Management Report.

Notification Options

Mail To:

SMS To: Click [here](#) to configure

Scheduling Options

Mail To:

Get Report for Every Day(s) @ Hrs Min For the

☒ PDF ☐ CSV

Test Now **Save** **Cancel**

The Firewall Analyzer fetches the Firewall device configuration on the following occasions:

- Device logout** - When ever Firewall Analyzer receives the device logout syslog
- Periodical** - The periodic schedule configured for fetching the device rules is applicable for fetching the configuration data also
- On Demand** - To fetch the configuration data when ever required, click **Settings > Device Rule** icon. It will open **Device Rule** page, in that page click the icon besides the '**View Config Changes**' link



While fetching configuration from the device for the first time, Firewall Analyzer will not set any pager to get the complete configuration data at one shot. Once the configuration is fetched, the pager is set to default. The default value of pager settings are given below:

- **Cisco:** 24 lines
- **Netscreen:** 20 lines
- **Fortigate:** No pager

Report Filter links

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown.

- Top 5
- Top 10
- Top 15
- Top 20
- Top 25

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Proxy Reports

Proxy Server Reports

The **Proxy Reports** section in Firewall Analyzer includes reports that are based on proxy cache logs. This section can be accessed from the left navigation pane or the **Reports** tab.

Squid is a widely used proxy cache for Linux and UNIX platforms. Squid is usually used together with a firewall to secure internal networks from the outside using a proxy cache.

In the latest release, Firewall Analyzer can receive the Syslogs live from the Proxy server (Squid). Now, it will parse and generate report. You can send Proxy server (Squid) logs using Linux Syslog daemon. To configure syslog service on Linux, refer the procedure given below.

It is now **optional** to configure Firewall Analyzer to import the Proxy server (Squid) logs at specific intervals.

The following reports are generated based on proxy cache logs:

- Live Reports
- Top Talkers
- Website Details
- Proxy Usage

Apart from these reports, **Live Reports** are available for proxy servers also. The Live Report for each proxy server shows the traffic load across the server, over different time periods.

Configuring the Syslog Service on a Linux/ UNIX Host

1. Login as root user and edit the **syslog.conf** file in the **/etc** directory.
2. Append ***.*<space>@<server_name>** at the end, where **<server_name>** is the name of the machine on which Firewall Analyzer is running.
3. Save the configuration and exit the editor.
4. Edit the **services** file in the **/etc** directory.
5. Change the syslog service port number to **514**, which is one of the default listener ports of Firewall Analyzer.
6. Save the file and exit the editor.
7. Restart the syslog service on the host using the command:
/etc/rc.d/init.d/syslog restart



For configuring **syslog-ng** daemon in a Linux host, append the following entries

```
destination firewallanalyzer { udp("<server_name>" port(514)); };
log { source(src); destination(firewallanalyzer); };
```

at the end of **/etc/syslog-ng/syslog-ng.conf**, where **<server_name>** is the ip address of the machine on which Firewall Analyzer is running.

Live Reports

The **Live Reports** provide a live visual representation of the traffic load across network links. Graphs are similar to that of MRTG, with the aim of providing a simple way to see exactly how much inbound and outbound traffic was generated for each device.

- Interface/Zone Reports For all devices
- Live Reports of Each Firewall Device
- Live Reports of Each Squid Device



SNMP base Live report graphs are not available for virtual Firewalls (vdom).

Interface/Zone Reports (Live Reports For all devices)

Click the **Interface/Zone Reports** link in the sub tab to see the Interface wise live reports for all devices, for the last 24 hours, over a 5-minute average.

Interface/Zone Live Reports Dashboard (Last 24 Hours) screen opens up. In that screen you will find **Device - Interface details** table. It will list all the devices and their interfaces. Click the **Show All** link or **+ tree** icon to the left of the device in the list. **Hide All** link or **- tree** icon will display the list of devices and the numbers of interface the device has. The expanded table lists the **Device Name**, **Interface Name**, **Bandwidth IN**, and **Bandwidth OUT**. Bandwidth IN and Bandwidth Out will display the bandwidth usage of the interface in percentage and the average speed in Kbps.

Click on the **Live Reports** link below the device in the list to view the live reports for that device alone.

Click on the individual interfaces names of the device in the list to view the only the live reports of the interface of the device.

Configure SNMP protocol settings for your Firewall device

The procedure to configure the SNMP protocol settings of Firewall devices in the Firewall Analyzer is given below:

- Click **Interface/Zone Reports > Click Configure SNMP protocol for Live reports. "Try now."** link. **Add Live Settings** page appears.
- In that, the devices are listed in the **Device Name** drop down list. Select the device as required.
- Below the **Device Name**, the **IP Address** of the selected device will appear.
- Select the **SNMP Version V1** or **V2** or **V3** using the respective radio button.
 - **Version 1 (V1):**
 - Enter the **SNMP Community** of the device in the text box
 - Enter the **SNMP Port** of the device in the text box
 - **Version 2 (V2):**
 - Enter the **SNMP Community** of the device in the text box
 - Enter the **SNMP Port** of the device in the text box
 - **Version 3 (V3):**

- Enter the **SNMP Community** of the device in the text box
- Enter the **SNMP Port** of the device in the text box
- Enter the **User Name** of the device in the text box
- Enter the **Context Name** of the device in the text box
- **Authentication:**
 - Select the **Protocol** for authentication from the drop down list (**MD5, SHA**).
 - Enter the **Password** for authentication in the text box
- **Encryption:**
 - Select the **Protocol** for encryption from the drop down list (**DES, AES**).
 - Enter the **Password** for encryption in the text box
- Select the reports in the **Select Reports** section. In that section, the **Report Name** and **Protocol** are listed.
- Select **Interface Live Report** using the check box. Select the **Protocol** for the report. On selecting the **Interface Live Report**, **Interval** field will appear with the drop down list. You can select **1 minute** or **5 minutes** or **10 minutes** granularity in Live reports by choosing appropriate interval.
- Select **Live VPN Users** report using the check box. Select the **Protocol** for the report. This report will be listed only if the device has the provision to get the Live VPN Users using SNMP protocol. Otherwise, this report option will not be there.
- The **Apply to other similar devices** section, contains list of devices of the same vendor type as the selected device with the check boxes to select, along with **Select All** devices option. If you want to apply the same credentials (Community, Port, etc..) to other similar firewalls, please select them.
- Click **Save** button to save the configuration and **Cancel** button to cancel the operation. Upon saving the form, the details are stored in the database and a sample SNMP query is made to test connection. If the SNMP credentials are not valid, you can skip saving the **Live Settings**.




If SNMP query is not successful, error message will be displayed on top of the page. Upon error, ensure the credentials provided are correct. Also ensure you have provided Management access through the source interface for SNMP protocol.


Once the '**Live Settings**' is added successfully, the **Edit | Disable | Delete SNMP** options are displayed to respective devices in **Interface Live Reports** Dashboard. The Live Reports and Interface Live Reports are populated with SNMP data.

Using the SNMP parameters configured, all the devices will be queried to get interface details. To configure/enable SNMP protocol in individual Firewall devices, refer the respective device configuration documents. Fortigate, Netscreen, Cisco PIX, Cisco ASA, Cisco Firewalls using ASDM tool

Once the SNMP settings is done for Live Reports, we skip the syslog data and use SNMP data for Live Reports. To switch to syslog option either disabling or deleting the SNMP settings. You could find this option to the right of device name in Interface/Zone Live Reports dashboard.

Configuring SNMP parameters for specific interfaces

Before the interface name, you will find  icon. Click the icon to set the **Interface Details** specific to this interface. **Configure Interface Details** screen pops-up. On the top you will see two options, one is **User Input** and the other is **Get from SNMP query** with radio buttons.

By default **User Input** radio button is selected. If you want to manually enter the interface details, carryout in this screen as given below: In the **User Input** screen, **Device Name**, **Interface Name** will be displayed. Besides the name of the interface, you will find  edit icon. Click the icon to change the interface name as per your requirement. The result will take effect immediately. You can enter the **Interface IP**, **Interface IP**, **Up Link Speed (in Kbps)**, and **Down Link Speed (in Kbps)** values manually.

Select the **Get from SNMP query** radio button if you want the application to automatically query the interface through SNMP and fetch the interface details. In the **Get from SNMP query** screen, **Device Name** will be displayed and you can enter the **Device IP Address**, **SNMP Community** and **SNMP Port**. Enter the the **SNMP Community** and **SNMP Port** parameters. Using the SNMP parameters configured, the specific interface will be queried to get interface details.

Click **Save** button to save the configuration and **Cancel** button to cancel the operation.



SNMP base Live report graphs are populated based on SNMP OID's ifInOctets and ifOutOctets. As these OID's are incremental counters we do not plot graph at a point when any of these counters gets reset.

Live Reports of Each Firewall Device

On the top right side of the Report screen, there will be two combo boxes. They are:

- Refresh
- Export as

Refresh

The **Refresh** combo box lets to enable or disable refreshing of the Live reports and lets you to choose the refreshing interval of the Live reports. There will be three field values for filtering. They are:

- Never Refresh
- Refresh Every 1 Min
- Refresh Every 5 Min
- Refresh Every 10 Min

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Click the **Live Reports** link present inside the list of reports for a device, to see the live reports for that device alone, over all the time periods described above.

The graphs for each device shows the minimum, maximum, and average amount of incoming and outgoing traffic through that device, over several time periods. Traffic is broken down into the last day, last week, last month, and last year, with an average granularity of 5 minutes, 30 minutes, 2 hours, and 1 day respectively.

The incoming and outgoing bandwidth can be viewed in Kbps.

Drill down from each of the graphs in the live report to see the following details:

Graph	Description
Inbound/Outbound Traffic Conversations	The inbound/outbound conversations for all hosts across this device. This data is available only for the last day's traffic over a 5-minute average granularity.
Top Hosts	The top hosts contributing to inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations for each host, during the selected time period.
Top Protocol Groups	The top protocol groups used in inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations using each protocol group, during the selected time period.
Top Users	The top users contributing to inbound/outbound traffic across this device. Drill down from this graph to see the corresponding conversations for each user, during the selected time period.



Live Reports will not be available for devices whose logs do not contain the "duration" field.

For example: *WatchGuard, SonicWall, Astaro, IP Filter Linux Firewall, etc...*

Live Reports of Each Squid Proxy Device

On the top right side of the Report screen, there will be two combo boxes. They are:

- Refresh
- Export as

Refresh

The **Refresh** combo box lets to enable or disable refreshing of the Live reports and lets you to choose the refreshing interval of the Live reports. There will be three field values for filtering. They are:

- Never Refresh
- Refresh Every 1 Min
- Refresh Every 5 Min
- Refresh Every 10 Min

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Click the **Live Reports** link present inside the list of reports for a device, to see the live reports for that device alone, over specific time periods.

The graphs for each device shows the minimum, maximum, and average amount of outgoing traffic through that device, over several time periods. Traffic is broken down into the last day, last week, last month, and last year, with an average granularity of 5 minutes, 30 minutes, 2 hours, and 1 day respectively.

The outgoing bandwidth can be viewed in Kbps.



Live Reports will not be available for devices whose logs do not contain the "duration" field.

Top Talkers

The **Top Talkers** section includes reports that show the top hosts and protocols generating traffic through the proxy server.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top LAN Hosts** and the **Top LAN Users** graphs show the respective top hosts and top users whose requests have been processed by the proxy cache itself. The table

below the graph shows the host name, IP address, or user name of the source, along with the protocol used, the number of hits, and the total traffic in bytes.

The **Top WAN Hosts** and the **Top WAN Users** graphs show the respective top hosts and top users whose requests could not be processed by the proxy cache. The table below the graph shows the host name, IP address, or user name of the source, along with the protocol used, the number of hits, and the total traffic in bytes.

The **Top Users (LAN + WAN)** shows the top values when the **Top LAN Users** and **Top WAN Users** records are combined. The table shows the User, the host name or IP address of the source from which he is conducting the conversation, the type of user (LAN or WAN) , the number of hits and bandwidth usage.

Drill down from each of the above graphs to see the following details:

Report	Description
Top Sites	The top web sites accessed by this user or host
Top Pages	The top web pages or URL's accessed by this user or host
Top Denied Web Pages	The top web pages that were denied for this user or host
Cache Usage - Cache Code	The cache usage by this user or host, based on cache code
Proxy Usage - HTTP Status Code	The proxy usage by this user or host, based on HTTP status code
Proxy Usage - Peer Status	The proxy usage by this user or host, based on peer status
Top Users/Hosts	The top users or hosts accessing the proxy through this host/user
Traffic Distribution - Working Hours	The amount of traffic that was generated during working hours, which is the daily average value since the time the server was started.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated after working hours, which is the daily average value since the time the server was started.

Website Details

The **Website Details** section includes reports that show the top domains, web sites, and web pages that were accessed using the proxy server.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Top Web Sites** report lists the top web sites that were accessed through this proxy server. This report classifies web sites based on the number of bytes that were transferred by a single user. Drill down from this graph to see the following details:

Report	Description
Top Users	The top users and the respective hosts accessing this web site
Top Web Pages	The top web pages accessed within this web site
Top Denied Web Pages	The top web pages in this web site that were denied
Cache Usage - Cache Code	The cache usage by web pages in this web site, based on cache code

The **Top Domains** report lists the top domains that were accessed through this proxy server. Drill down from this graph to see the following details:

Report	Description
Top Users	The top users and the respective hosts accessing this domain
Top Web Pages	The top web pages accessed within this domain
Top Denied Web Pages	The top web pages in this domain that were denied
Cache Usage - Cache Code	The cache usage by web sites in this domain, based on cache code

The **Top Web Pages** report lists the top web pages or URL's that were accessed through this proxy server, along with the number of hits and the total traffic sent to each web page, in bytes. This report classifies web pages based on the number of bytes that were transferred by a single user.

The **Top Denied Users** report lists the top users whose requests were denied by this proxy server. Drill down from this graph to see the top denied requests for each user.

The **Top Denied Requests** report shows the top requests that were denied by the proxy server.

Proxy Usage

The **Proxy Usage** section includes information about the cache usage and proxy usage of the proxy server.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol
- Summary

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Cache Usage - Cache Code** report shows the top cache result codes triggered. This report help you analyze the efficiency and performance of the proxy server. A high number of TCP_DENIED hits for example, could indicate that most users in the network

are trying to access unauthorized resources, or are simply unaware of present network security policies. Drill down from this graph to see the following details:

Report	Description
Top Hosts	The top hosts and users that triggered this cache result code
Top Web Pages	The top web pages that triggered this cache result code

The **Proxy Usage - Peer Status Code** report shows the top peer status codes triggered. This report shows you the number of requests that were generated directly from the origin, and how many were passed from another source. Drill down from this graph to see the following details:

Report	Description
Top Hosts	The top hosts and users that triggered this peer status code
Top Web Pages	The top web pages that triggered this peer status code

The **Proxy Usage - HTTP Status Code** report shows the top HTTP status codes triggered, like 200, 404, etc...

The **Proxy Usage - HTTP Operation** report captures the various operations like get, post, connect, etc..

All the above reports classify values based on the number of times each code was triggered.

Proxy Server - URL Categories Reports

The **URL Categories Reports** section includes reports on the categories of URL fetched from the Proxy server logs. The logs contain the URL category information and the number hits on the URL categories. In the **URL Categories Report: <Proxy Server>**, the graph and the table lists the categories and the hits of **Top Allowed Categories** and **Top Denied Categories**. Click on the particular category of allowed or denied categories, to view the **Category Drill Down Report**. The **Category Drill Down Report** lists the **Top URLs**, **Top Sources** and **Top Destinations** of a particular category.

On the top right side of the Report screen, there will be three combo boxes. They are:

- Top 5
- Filter by
- Export as

Top 5

The **Top 5** combo box lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than 15 values, the report uses only tables. There is an option to display the Graph only.

- Top 5 (graph & table)
- Top 10 (graph & table)
- Top 15 (table only)
- Top 20 (table only)
- Top 25 (table only)
- Graph only

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

Filter by

The **Filter by** combo box lets you choose the field of filter in the reports. There will be three field values for filtering. They are:

- Source
- Destination
- Protocol

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

The **Category Drill Down Report** lists the **Top URLs**, **Top Sources** and **Top Destinations** of a particular category.

The **Top URLs accessed under <category> Category** table lists the URLs accessed under the particular category. The table shows the list of URLs accessed under the particular category and the number of hits.

Graph	Description
URLs	The list URLs accessed under the particular category
Hits	The number of hits for each URL under the particular category

The **Top Sources for <category> Category** table lists the URLs accessed under the particular category. The table shows the list of hosts from where the URLs were accessed under the particular category and the number of hits.

Graph	Description
Hosts	The list of hosts from where the URLs were accessed under the particular category
Hits	The number of hits for each URL under the particular category

The **Top Destinations for <category> Category** table lists the URLs accessed under the particular category. The table shows the list of destination in which the URLs were accessed under the particular category and the number of hits.

Graph	Description
Destinations	The list of destination in which the URLs were accessed under the particular category
Hits	The number of hits for each URL under the particular category

Trend Reports

Trend Reports analyze traffic over several time periods and present graphs that make analysis and forecasting a lot easier. Firewall Analyzer includes trend reports based on traffic generated, protocols used, and events triggered. Trend reports compare the current trend with the historical trend on an hourly, daily, and weekly basis. Historical trends show data from the time the server was started.

Firewall Analyzer includes three types of trend reports that are described in the following sections:

- Protocol Trend Reports
- Traffic Trend Reports
- Event Trend Reports
- VPN Trend Reports

Protocol Trend Reports

The **Protocol Trend Reports** section includes reports that show trends in the amount of traffic generated using different protocol groups. Protocol trends help in identifying peak usage times for each protocol group, understanding user trends, and enforcing better policies to allow traffic from each protocol group.

On the top right side of the Report screen, there will be a drop down menu.

- Export as

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

The **Hourly Trend Comparison** reports for Web, Mail, FTP, and Telnet protocol groups compare the traffic generated using these protocol groups over the past day, with the traffic generated since the time the server was started.

The **Working Hour** and **Non-working Hour Traffic Trend** reports show the amount of traffic generated using each protocol group during working and non-working hours respectively, since the time the server was started.

Traffic Trend Reports

The **Traffic Trend Reports** section includes reports that show trends in the amount of traffic generated across the firewall. Traffic trends help in understanding peak usage times, enforcing better security policies, and planning for effective bandwidth upgrades. In a large enterprise with several firewalls, traffic trends can also help the network administrator to distribute the traffic load between firewalls to reduce response times and thereby enable better quality of service.

On the top right side of the Report screen, there will be a drop down menu.

- Export as

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

The **Hourly Trend Comparison** report compares the amount of traffic generated across this firewall over the past day, with the amount of traffic generated across this firewall since the time the server was started.

The **Weekly Trend Comparison** report compares the amount of traffic generated across this firewall over the past week, with the amount of traffic generated across this firewall since the time the server was started.

The **Working Hour** and **Non-working Hour Traffic Trend** reports show the amount of IN and OUT traffic generated across this firewall during working and non-working hours respectively, since the time the server was started.

Event Trend Reports

The **Event Trend Reports** section includes reports that show trends in the number of events generated across the firewall. Event trends help in identifying malfunctioning hosts and malevolent systems, that eventually lead to enforcing better security policies, and increasing network perimeter security.

On the top right side of the Report screen, there will be a drop down menu.

- Export as

Export as

The **Export as** combo box lets you choose the format of the reports for export. There will be two formats for exporting. They are:

- PDF
- CSV

Click on the PDF to export this report to PDF. Click on the CSV to export this report to CSV format (comma separated values).

Below each graph click the **Hide Table** link to hide the table. Click the **Show Table** link to see the table again.

The **Hourly Trend Comparison** report compares the number of events generated across this firewall over the past day, with the number of events generated across this firewall since the time the server was started.

The **Weekly Trend Comparison** report compares the number of events generated across this firewall over the past week, with the number of events generated across this firewall since the time the server was started.

The **Working Hour** and **Non-working Hour Event Trend** reports show the number of events generated across this firewall during working and non-working hours respectively, since the time the server was started.

VPN Trend Reports

VPN trends help in identifying VPN connections spread over a time period for a particular device, that eventually lead to better planning of VPN policies, and increasing the VPN usage efficiently. The **VPN Trend Reports** section includes reports that show trends in the number of VPN users connecting across the Firewall/Concentrator.

The VPN Trend Report consists of two parts. On the top, the list of VPN users currently active are listed as **Live VPN Users** and below that the time based trend reports of VPN usage are displayed in graphs as **VPN Trends**.

Live VPN Users

Details of all the VPN Users currently connected across the Firewall/Concentrator are listed in this section of the report.

The details in the **Live VPN Users** list are explained below:

VPN User	- the user name of the VPN connection across firewall.
Host	- the host name / IP address of the machine of the VPN user, which got connected through VPN.
VPN Type	- the type of VPN connection used by the user.
Start Time	- the time at which the VPN connection across firewall for the user was started.
Duration	- the duration of time up to the current time, for which the user is connected through VPN across firewall.

VPN Trends

The VPN trend reports are available separately for each Firewall/Concentrator device. These are pre-defined reports. There are four trend reports available for VPN. They are:

1. Last 24 Hours VPN Trend
2. Last 7 Days VPN Trend
3. Last 30 Days VPN Trend
4. Last Year VPN Trend

The description of the VPN trend reports are given below:

The **Last 24 Hours VPN Trend** report compares the number of VPN user connections across this firewall over the past 24 hours, with the time in hours at the X axis of the graph always representing the last 24 hours prior to the current time.

The **Last 7 Days VPN Trend** report compares the number of VPN user connections across this firewall over the past 7 days, with the day at the X axis of the graph always representing the last 7 days prior to the current date.

The **Last 30 Days VPN Trend** report compares the number of VPN user connections across this firewall over the past 30 days, with the date at the X axis of the graph always representing the last 30 days prior to the current date.

The **Last Year VPN Trend** report compares the number of VPN user connections across this firewall over the past 12 months, with the month at the X axis of the graph always representing the last 12 months prior to the current month.

Custom Reports

Creating Report Profiles




Custom reports in Firewall Analyzer are grouped into report profiles, and listed under the **My Reports** category. A report profile can contain a combination of pre-defined and custom reports. The **My Reports** section is present in the **Reports** tab and the left navigation pane.

The **My Reports** section lists all the custom reports created so far, the hosts that are reported on, and scheduling options. Click on the report name to view the report. The page contains a menu bar and the menu bar contains the following menu:

- **Add Report Profile** - Click this menu to create a new custom report.
- **Delete Report** - Select the check boxes of custom reports to be deleted and click the **Delete Report** link to delete report(s).
- **Export Report Profiles** - Select the check boxes of report profiles to be exported and click this menu. The profile will be downloaded as an XML file (**FirewallAnalyzer_Profiles.xml**), through your browser into your client machine.
- **Import Report Profiles** - Click this menu to import report profiles. On clicking the menu, **Select Report Profiles file to import:** screen pops-up. In that, you will find **File Location** text box and **Browse** button besides. Enter the location of the XML file (**FirewallAnalyzer_Profiles.xml**) or use the browse button to locate the XML file. Click **Import** button to import the profiles in to Firewall Analyzer server and **Cancel** button to cancel the import profiles operation. If the report already exist in Firewall Analyzer, clicking **Import** button will list **Failed To Import** option and the existing reports with check boxes and you will find **Over Write** button and **Cancel** button to cancel the import profiles operation. Select the check boxes of report profiles to overwrite and click **Over Write** button.



There will be no hosts configured for the imported report profiles. You have to edit the report profile to configure the hosts.

Click the  icon to edit the corresponding custom report configuration details. If the report profile has no schedules associated with it, the  icon is displayed. Click this icon to schedule the report profile. If the report profile already has a schedule associated with it, the  icon is displayed. Click this icon to create another schedule for this report profile.

The process of creating a report profile includes several other tasks such as including and excluding log filters, and setting custom criteria for specific reports.

If Include/Exclude Log Filters are applied to a custom report profile, it will be displayed with an icon and **Filter Applied** link on top of the reports display of the profile.

Creating a Report Profile

Click the **Add Report Profile** link to create a new report profile. You can click this link from the sub tab, the left navigation pane, or the **My Reports** section in the **Reports** tab.

Step 1: Select Devices and Filters


1. For **Report Profile Name**, enter a unique name for the report profile.
2. Select the **'Want to assign this profile to any 'Guest' privilege user'** check box, if you want to assign this profile to a guest user to view. On selecting the check box, the drop down box containing the 'Guest' privilege users


appears besides the selection. Select the specific user to whom you want to assign this profile to view. This option is useful for MSSPs and large enterprises, where the user demands a report and confirm the report profile solves the purpose.


3. Select the devices (firewalls, squid, ...) to report on. If you want to report on all the devices sending logs to a specific syslog port, then select the **Select All Devices** check box.
4. You can specify the filters on log data, in the section **Choose the Filters**. Follow the instructions available for Setting Log Filters to know more about operations on Include and Exclude filters.
5. Click **Next** to continue to the next step of the wizard. Click **Cancel** to exit the wizard.

Step 2: Select Report Type and Schedule

This step lets you specify which reports to include as part of this report profile, and set up schedules to generate this report profile automatically.

1. From the list of **Available Reports**, select the reports that you want to include in this report profile. All the pre-defined reports are listed, along with custom reports that you have previously set up. Below the **Available Reports** list, **Add**  link with icon is available to create custom report. Clicking the link, opens the Define New Report screen pops up.

	Look up Define New Report to know more about adding a new report to this list
---	---

2. You can save the report in PDF and also can customize the PDF report by selecting the **Customize images for PDF Reports**, whereby you can provide your own **Cover image** (820 by 612 pixels) and **Footer image** (37 by 547 pixels).
3. In the **Schedule & Email Options** section, choose the format of report to be Emailed using **Send report as: PDF CSV** radio buttons. Choose a **Schedule Type** to schedule this report to be automatically generated at specific time intervals. Choose from *hourly*, *daily*, *weekly*, or *monthly* schedules, or choose to run this report *only once*. For **Daily**, and **Only once** schedules, you can set the  **TimeFilter** for **Custom Hours**, **Only Working Hours**, or **Only NonWorking Hours**.

For the **Daily** schedules, if the option **Run on Week Days** is selected then the reports are run daily except on the weekends. For the **Weekly** or **Monthly** schedules, select the option **Generate Report only for Week Days** if you want to report on the events that occurred only on the week days and not report on events that occurred over the weekends.

If the **Email the Report** option is checked, the scheduled report will be generated and emailed as PDF to the **Mail Id** that is provided. You can use comma "," separator for multiple mail ids.




You need to configure the mail server settings in Firewall Analyzer before setting up an email notification. You can do this from the **Setup the Mail-Server Details** link.

4. Click **Preview** to see how this report will look like, once it is set up. Click **Save** to save this report profile under the **My Reports** section. Click **Cancel** to exit the wizard.


Setting Log Filters

Include filters specify those criteria which the log data must meet in order to be included in the report. *Exclude* filters specify those criteria which the log data must meet in order to be excluded from the report. Apart from selecting specific filters to apply on a report, you can also add, select, edit, and delete filters in this step. Include and Exclude filters let you filter log data and show only specific details in the custom report. Once you have set filters, you can include or exclude them while creating custom reports.


Adding a New Filter:

1. Click the  Add icon to add a new filter
2. In the popup window that opens, enter a unique name for the filter
3. Select the type of filter you are creating, whether its a **Include Filter** or an **Exclude Filter**.
4. In the **Include the following Protocols** drop-down, choose the protocols to be filtered
5. In the **Include the following IP/Hostname** drop-down, specify the IP addresses of the hosts (Single or IPRange or CIDR) to be filtered.
6. In the **Include the following Destinations** drop-down, specify the IP addresses of destination address (Single or IPRange or CIDR) to be filtered
7. In the **Include the following Events** drop-down, choose the event priorities to be filtered
8. In the **Include the following Users** text box, specify the users to be filtered. In this, you can use standard wild card characters for easy filtering.
9. Click **Finish** to create the new filter. Click **Cancel** to exit the wizard without saving the new filter.


Selecting a Filter:

1. Click the  Select icon to select from the list of already created filters.
2. You can select a specific filter or **All filters** and then click the **Select** button. Click **Cancel** to exit the wizard without selecting.

Editing a Filter:



1. Click the  Edit icon to edit an existing filter
2. Editing a filter affects all existing report profiles to which this filter is applied. If you still want to edit the filter, accept the warning message and proceed editing.
3. The wizard for editing the filter is similar to that for adding a new filter. Follow the same steps and click **Finish** to save the edited filter. Click **Cancel** to exit the wizard without saving the edited filter.


Removing a Filter:

1. Click the  Remove icon to remove or delete an existing filter
2. Choose whether you would like to **Remove filter from the list** or **Remove it completely**
3. **Remove filter from the list** option will only remove the filter from this listing, but would still be available for selection. **Remove it completely** option will remove this filter permanently and affects all existing report profiles to which this filter is applied. If you still want to remove this filter completely, accept the warning message. The filter is removed, and all report profiles to which this filter is applied, are permanently modified to reflect the changes.

Creating Custom Criteria Reports

Firewall Analyzer lets you define custom criteria and set up new reports. These reports are added to the Available Reports list, in Step 2 of the **Add Report Profile** wizard.

1. In Step 2 of the **Add Report Profile** wizard, click the  icon to add a new report
2. In the **Define New Report** popup window that opens, enter a unique name for the report in the **Report Name** field.
3. In the **Report based on** selection, choose *Protocol, URL, Event, VPN, Rule, Attack, Virus, Spam, Host, Server* depending on the report criteria you want to specify.
4. In the **Display** option, select one of the three options: *Graph & Table, Graph, Table*.
5. In the **Graph Settings** tab, choose the following:
 1. The type of graph to be displayed, in the **Graph Types** drop-down list. The **Graph Types** are: *Vertical Bar Chart, Vertical 3-D Bar Chart, Stacked Vertical Bar Chart, Horizontal Bar Chart, Horizontal 3-D Bar Chart, Stacked Horizontal Bar Chart, Pie Chart, 3-D Pie Chart, Time Series*. A preview of the graph will be available besides the **Graph Types** selection. The **Time Series** graph will give Time Vs any of attributes: *Hits, Total Bytes, Bytes Sent, Bytes Received*.
 2. The attributes to be used for the X and Y axes of the graph, along with the labels to be displayed. The **Y-axis** attributes are: *Sum of Bytes Received, Sum of Total Bytes, Sum of Bytes Sent, Sum of Request Count, Sum of Duration* and the **X-axis** attributes are: *Resource, Source, User, Destination, Protocol, Time, Duration, Request Count, Bytes Received, Bytes Sent, Total Bytes*.
 3. The attribute based on which all data will be grouped together, in the **Grouping Criteria** option. The options are: *Resource, Source, User, Destination, Protocol, Time*. Click  icon to **Add Secondary 'Group By' option**, this will be useful for generating Stacked Graphs report.
 4. The attribute based on which data will be sorted, in the **Order By** option. The options are: *Sum of Bytes Received, Sum of Total Bytes, Sum of Bytes Sent, Time, Sum of Request Count, Sum of Duration*.
6. In the **Table Settings** tab, choose the values to be shown in the table of the report. Select from the **Available Headers** table and click **>>** button to the header to **Selected Header** table. The values of the selected headers will be displayed in the table.
7. Once you have selected all the required options, click **Apply** to include this new report in the Available Reports list. Select the checkbox next to this report to include it in a report profile.

You can click the  icon at any time to delete a custom report from the Available Reports list.

Using Advanced Search

Firewall Analyzer provides advanced search feature. Advanced Search, offers numerous options for making your searches more precise and getting more useful results. It allows you to search from the Raw Firewall Logs. Using this feature, you will be able to save the search results as Report Profiles. This provides a simplified means to create very precise, selectively filtered and narrowed down Report Profiles.

- Advanced Search
- Using Advanced Search to create Report Profiles

Advanced Search

In Advance Search, you can search the logs for the selected devices, from the aggregated logs database or raw firewall logs, and define matching criteria.

Selected Devices

In this section, you can choose the devices for which you want the logs to be searched. If no device is selected or you want to change the list of selected devices, select the devices.

1. Click **Change Selection** link.
2. **Select Devices from the list** window pops-up. In that window, All Devices with selection check box and individual devices with selection check boxes options are available.
3. Select the devices by selecting the check boxes as per your requirement. Click **OK** to select the devices and close the window or click **Cancel** to cancel the operation and close the window.

The selected devices are displayed in this section.

Search From

In this section, you can select one from the two options:

1. Aggregated Logs Database
2. Raw Firewall Logs

1. Aggregated Logs Database

Select this option if you want to search from the aggregated logs database.

2. Raw Firewall Logs

Select this option if you want to search from the raw firewall logs. Selecting this option will enable the following options:

- a. **Raw VPN Logs**
- b. **Raw Virus/Attack Logs**
- c. **Raw Device Management Logs**
- d. **Raw Denied Logs**

Select the above logs options as per your requirement.

Define Criteria

This section, enables you to search the database for attributes using more than one following criteria's:

Criteria	Description
Protocol	Refers to the list of protocols and protocol identifiers that are available in the Protocol Groups page (Settings >> Protocol Groups) <i>example: 8554/tcp, rtsp, IPSec</i>
Source	Refers to the source host name or IP address from which requests originated
Destination	Refers to the destination host name or IP address to which requests were sent
User	Refers to the authenticated user name required by some firewall's <i>example: john, kate</i>
Virus	Refers to the Virus name. <i>examples: JS/Exception, W32/Mitglieder</i>
Attack	Refers to the attack name. <i>examples: UDP Snort, Ip spoof</i>
Device	Refers to the device from which logs are collected
Message	Refers to the log message texts stored in the DB

- If the search string exists then the search result will be intelligently displayed based on the report category in which it occurred.
- By default, the search is carried out for the time period selected in the Global Calendar present in the left pane of the UI.
- You can also search within the search results.

Using Advanced Search to create Report Profile


To generate remote VPN users reports:

- Click **Advanced Search** link in the Sub Tab.
- Select appropriate Devices.

Raw Firewall Logs

- Select **Raw Firewall Logs** radio button.
- Select **Raw VPN Logs** in the Raw Firewall Logs group.
- In the **Criteria** section, enter **Duration** *isn't '0'*.
- Click **Search** and click **Configure Columns** to change reports columns.

Aggregated Logs Database

- Select **Aggregated Logs Database** radio button.
- In the **Criteria** section, select **Match all of the following** or **Match any of the following** to match all the criteria set or any of the criteria set and add or remove additional criteria using **Add Criteria** and **Remove Criteria** links and select **Protocol is 'HTTP'**.
- Click **Search**. Search results provide the *Reports related to your search <for time period from beginning of the day to current time>*.
- Select the required reports by selecting the individual reports or by selecting the **Add Criteria** to select all the reports. These will form the criteria for the Report Profile.
- To save the search result as report profile, click **Save as Report Profile** link.
- Enter a **Report Profile Name**.
- Schedule the report, if required by selecting **Associate Schedule** check box.
- In the **Schedule & Email Options** section, choose the format of report to be Emailed using **Send report as: PDF CSV** radio buttons. Choose a **Schedule Type** to schedule this report to be automatically generated at specific time intervals. Choose from *hourly, daily, weekly, or monthly* schedules, or choose to run this report *only once*. For **Daily**, and **Only once** schedules, you can set the  **TimeFilter** for **Custom Hours**, **Only Working Hours**, or **Only NonWorking Hours**.

For the **Daily** schedules, if the option **Run on Week Days** is selected then the reports are run daily except on the weekends. For the **Weekly** or **Monthly** schedules, select the option **Generate Report only for Week Days** if you want to report on the events that occurred only on the week days and not report on events that occurred over the weekends.

If the **Email the Report** option is checked, the scheduled report will be generated and emailed as PDF to the **Mail Id** that is provided. You can use comma "," separator for multiple mail ids.



You need to configure the mail server settings in Firewall Analyzer before setting up an email notification. You can do this from the **Setup the Mail-Server Details** link.

- Click **Save as Profile** button. A new report profile is added.



In the Configure Columns pop-up screen you can select the required columns of the report. For example: User, StartTime, Time, and Duration. Here, Time represents EndTime of the VPN connection.

Notifications

Creating an Alert Profile

An alert is triggered whenever an event matching a specific criteria is generated. An alert profile lets you define such specific criteria, and also notify you by email, when the corresponding alert is triggered.

- Creating New Alert Profile
- Example Alert Profile

Creating a New Alert Profile

Click the **Add Alert Profile** link to create a new alert profile. You can find this link on the sub tab or in the **Alerts** box in the left navigation pane when the **Alerts** tab is selected.

1. Enter a unique name for the alert profile in the **Profile Name** field.
2. Select the **Profile Type**:
 - a. **Normal Alert Profile**
 - i. **Select Device(s)** for which the alert needs to be triggered by selecting the **Select All** check box or selecting the check boxes of required devices.
 - ii. **Criteria** for which the alert needs to be triggered. You can use the logical and/or of the selected criteria using **Match all of the following** or **Match any of the following** selections. You can set criteria based on the Severity, Protocol, Date, Received (in Bytes), Sent (in Bytes), Source, User, Destination, URL, Status, File Name, Rule, VPN, Virus, Attack, Protocol Identifies, Message, Duration (in seconds), Record Type, Log ID, Category. Use the **Add** and **Remove** links to specify more or fewer criteria for the alert.
 - iii. **Threshold**:
The **Priority** of the alert can be *High*, *Medium*, or *Low* based on your requirement for notification. Select the appropriate Priority.
 - iv. Enter the threshold criteria for the alert to be triggered.
For example: *Alert for every: 5 Events generated within 2 Minutes*
Here, *Events* refer to the criteria that has been defined above.
 - v. Select the owner for the alert from the **Assign Owner**: combo box. The combo box lists all the available users in the Firewall Analyzer.
 - vi. You can **Apply Threshold to**:
Either, **All Devices Selected**, in which case the alert will be triggered when all the firewalls cumulatively crosses the threshold set in the threshold criteria above.
Or, **Each Device Selected**, in which case the alert will be triggered when each firewall crosses the threshold set in the threshold criteria above.
 - vii. **Notification**:
Select the check box **Send the notifications once and do not send for <This Day, This Week, This Month, Custom Period>**, to send only one alert notification for the selected period, irrespective of any number of alerts generated during the selected

- period. Custom Period selection will display **_ Days, _ Hours, _ Mins** fields besides the selection list.
- b. **Anomaly Alert Profile** type, can be selected when you would like to be notified of any **abnormal** behaviors or traffic anomalies. Anomaly reports can be used for Network Behavioral Analysis (NBA).
 - i. **Select Device(s)** for which the alert needs to be triggered by selecting the **Select All** check box or selecting the check boxes of required devices.
 - ii. Select the type of anomaly alert report (**Anomaly Report Type**) you would like to receive. The report types could be Traffic Report, Attack Report, Virus Report, VPN Report, URL Report, Rule Report, or Event Report.
 - iii. **Filters:**
Each of the above report types provide a set of filters which can be configured as per the nature of the alert you would like to receive.
 - iv. **Threshold:**
Based on the anomaly report type and corresponding filter you have chosen, the threshold criteria for the alert to be triggered can be set here.
 - v. Select the owner for the alert from the **Assign Owner:** combo box. The combo box lists all the available users in the Firewall Analyzer.
 - vi. **Notification:**
Select the appropriate radio button in **Send the below notifications on every 1st 2nd 3rd 4th 5th occurrence** option. Select the check box **Send the notifications once and do not send for <This Day, This Week, This Month, Custom Period>**, to send only one alert notification for the selected period, irrespective of any number of alerts generated during the selected period. Custom Period selection will display **_ Days, _ Hours, _ Mins** fields besides the selection list.

Anomaly Sample Scenario :

In a period of 1 hour, if traffic from source 192.168.1.1 exceeds 100 MB, create a High Priority Alert and send me an email notification on every 5th occurrence. Also, once in 15 minutes, check whether the traffic has exceeded 100 MB.

You can achieve the above scenario using the Anomaly Filters.

Steps:

7. **Filters** section:
Give **Source is 192.168.1.1**
8. **Threshold** section:
In a period of **1 Hour**, If **Total Traffic** exceeds **100 MB**, create an Alert with Priority as **High** Check for every **15Mins**. Select the owner for the alert **<Admin>** from the **Assign Owner for the Alert:** combo box.
9. Select **Send E-Mail notification** check box and select **5th occurrence**. Provide valid email ids in the **Mail To** box.

Example:

You will get an email when the following example values are met in your Firewall Analyzer.

Schedule Time	Time Range	Total Bytes (MB)	Alert	Email
10th Aug 10:00	9:00 to 10:00	104	YES	NO
10th Aug 10:15	9:15 to 10:15	106	YES	NO
10th Aug 10:30	9:30 to 10:30	200	YES	NO
10th Aug 10:45	9:45 to 10:45	167	YES	NO
10th Aug 11:00	10:00 to 11:00	154	YES	YES

Schedule Time: Time at which Firewall Analyzer checks the database to identify the amount of traffic from Source 192.168.1.1

Time Range: Time period for which the traffic is examined

Total Bytes (MB): Actual bytes transferred from 192.168.1.1

Alert: Does Firewall Analyzer report Alert or not?

Email: Does Firewall Analyzer send E-Mail or not?

C. Bandwidth Alert Profile

- i. **Select Device** for which the interface bandwidth alert needs to be triggered by selecting the radio button of the live SNMP settings configured devices. Only SNMP Live Settings configured devices will be listed for the Bandwidth Alert selection.
 - ii. **Criteria** for which the alert needs to be triggered. You can set criteria based on the *inside* or *outside* interface of the device, *Inbound traffic*, *Outbound traffic*, *Total traffic* and \geq or \leq and _ **bps** or **%**. Use the +, X buttons to specify more or fewer criteria for the alert. If more than one criteria is selected, no two criteria can have the same interface (*inside* or *outside*)
 - iii. Threshold:
The **Priority** of the alert can be *High*, *Medium*, or *Low* based on your requirement for notification. Select the appropriate Priority.
 - iv. Enter the threshold criteria for the alert to be triggered.
For example: *Alert for every: 5 Events generated within 2 Minutes*
Here, *Events* refer to the criteria that has been defined above.
 - v. Select the owner for the alert from the **Assign Owner:** combo box. The combo box lists all the available users in the Firewall Analyzer.
 - vi. Notification:
Select the check box **Send the notifications once and do not send for <This Day, This Week, This Month, Custom Period>**, to send only one alert notification for the selected period, irrespective of any number of alerts generated during the selected period. Custom Peiod selection will display _ **Days**, _ **Hours**, _ **Mins** fields besides the selection list.
3. There is a provision to receive a HTML mail containing the alert details, every time an alert matching this alert profile is triggered, select the **Send E-mail Notification** checkbox. Fill in the recipient email address in the Mail To box. Emails can be sent to more than one email address by separating the email addresses using a comma (.).



You need to configure the mail server settings in Firewall Analyzer before setting up an email notification.

5. There is a provision to execute custom scripts, every time an alert matching this alert profile is triggered, select the **Run Script** checkbox. **Enter Script Location** section appears below the option. Specify the location of the script to be executed in the Location field. Alternatively, use the **Browse** button to locate the script. The parameters of the log can be passed as arguments to the script to be executed. Click **+Add** link to select the parameters to be added in the Arguments field. The list of parameters with check boxes are displayed in a pop-up screen. Select the required parameters and close the screen. You can also specify other arguments as required. If the argument value is not available in the matching log, '-' character will be substituted.
6. There is a provision to receive SMS message in your mobile phone containing the alert details, every time an alert matching this alert profile is triggered, select the **Send SMS Notification** checkbox. Fill in the recipient mobile phone number with country code. SMS cannot be sent to more than one phone number.



You need to configure the SMS settings in Firewall Analyzer before setting up an SMS notification.

7. Click **Save Profile** button to save the alert profile.

Filters for various Alert Reports

Filters common to all Report types:

- **Time** filter values are *Working Hours*, *Non Working Hours*, *Week Days*, *Week Ends* and the default value is *No Criteria*. Select the Time value
- **Source** filter conditions are *Is*, *Is Not*, *Contains*, *Starts With* and *Ends With*. Enter source name. If you want to enter multiple values, use CIDR or CSV formats.
- **Protocol** filter conditions are *Is*, *Is Not*, *Contains*, *Starts With* and *Ends With*. Enter protocol.
- **Destination** filter conditions are *Is*, *Is Not*, *Contains*, *Starts With* and *Ends With*. Enter destination name. If you want to enter multiple values, use CIDR or CSV formats.

Traffic Report:

- Time
- Source
- Protocol
- Destination
- User filter conditions are *Is*, *Is Not*, *Contains*, *Starts With* and *Ends With*. Enter user name for which you want the alert to be generated.

Attack Report:

- Time
- Source
- Protocol

- Destination ?
- Attack filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the attack name for which you want the alert to be generated.
- Message filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the message part or whole for which you want the alert to be generated.
- Severity filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the severity of the attack for which you want the alert to be generated.

Virus Report:

- Time ?
- Source ?
- Protocol ?
- Destination ?
- Virus filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the VIRUS name for which you want the alert to be generated.
- Message filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the message part or whole for which you want the alert to be generated.
- Severity filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the severity of the Virus for which you want the alert to be generated.

VPN Report:

- Time ?
- Source ?
- Protocol ?
- Destination ?
- User filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter user name for which you want the alert to be generated.
- VPN filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the VPN connection for which you want the alert to be generated.

URL Report:

- Time ?
- Source ?
- Protocol ?
- Destination ?
- User filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter user name for which you want the alert to be generated.
- URL filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the URL for which you want the alert to be generated.
- Category filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the URL category for which you want the alert to be generated.

Rule Report:

- Time ?
- Source ?

- Protocol ?
- Destination ?
- User filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter user name for which you want the alert to be generated.
- Rule filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter rule name for which you want the alert to be generated.
- Message filter conditions are *Is, Is Not, Contains, Starts With* and *Ends With*. Enter the message part or whole for which you want the alert to be generated.

Threshold for various Alert Reports

Threshold common to all Report types:

Show Trend

Assign Owner - Select the owner for the alert from the **Assign Owner**: combo box. The combo box lists all the available users in the Firewall Analyzer.

Check for every 15 Mins, 30 Mins, 1 Hour, 2 Hours, 6 Hours, 12 Hours

Traffic Report:

- **In a period of** 1 Hour, 2 Hours, 6 Hours, 12 Hours, 1 Day, 7 Days, 14 Days, 30 Days, This Week, This Month **If** Total Traffic, Sent Traffic, Received Traffic, Number of Hits, Duration **of** All, Any Source, Any Destination, Any Protocol **exceeds** <amount>_ MB, GB, KB or Times or secs, minutes, hours, days.
- create an Alert with Priority as - **Priority** of the alert can be *High, Medium*, or *Low* based on your requirement for notification. Select the appropriate Priority.
- **Assign owner** ?
- **Check for every** ?

Attack Report:

- **In a period of** 1 Hour, 2 Hours, 6 Hours, 12 Hours, 1 Day, 7 Days, 14 Days, 30 Days, This Week, This Month **If** Number of Hits **of** All, Any Source, Any Destination, Any Protocol **exceeds** <number>_ times.
- create an Alert with Priority as - **Priority** of the alert can be *High, Medium*, or *Low* based on your requirement for notification. Select the appropriate Priority.
- **Assign owner** ?
- **Check for every** ?

Virus Report:

- **In a period of** 1 Hour, 2 Hours, 6 Hours, 12 Hours, 1 Day, 7 Days, 14 Days, 30 Days, This Week, This Month **If** Number of Hits **of** All, Any Source, Any Destination, Any Protocol **exceeds** <number>_ times.
- create an Alert with Priority as - **Priority** of the alert can be *High, Medium*, or *Low* based on your requirement for notification. Select the appropriate Priority.
- Assign owner ?
- Check for every ?

VPN Report:

- **In a period of** *1 Hour, 2 Hours, 6 Hours, 12 Hours, 1 Day, 7 Days, 14 Days, 30 Days, This Week, This Month* **If** *Total Traffic, Sent Traffic, Received Traffic, Number of Hits, Duration* **of** *All, Any Source, Any Destination, Any Protocol* **exceeds** *<amount>_ MB, GB, KB or Times or secs, minutes, hours, days.*
- create an Alert with Priority as - **Priority** of the alert can be *High, Medium, or Low* based on your requirement for notification. Select the appropriate Priority.
- **Assign owner** ?
- **Check for every** ?

URL Report:

- **In a period of** *1 Hour, 2 Hours, 6 Hours, 12 Hours, 1 Day, 7 Days, 14 Days, 30 Days, This Week, This Month* **If** *Total Traffic, Sent Traffic, Received Traffic, Number of Hits, Duration* **of** *All, Any Source, Any Destination, Any Protocol* **exceeds** *<amount>_ MB, GB, KB or Times or secs, minutes, hours, days.*
- create an Alert with Priority as - **Priority** of the alert can be *High, Medium, or Low* based on your requirement for notification. Select the appropriate Priority.
- **Assign owner** ?
- **Check for every** ?

Rule Report:

- **In a period of** *1 Hour, 2 Hours, 6 Hours, 12 Hours, 1 Day, 7 Days, 14 Days, 30 Days, This Week, This Month* **If** *Number of Hits, Denied Requests* **of** *All, Any Source, Any Destination, Any Protocol* **exceeds** *<number>_ times.*
- create an Alert with Priority as - **Priority** of the alert can be *High, Medium, or Low* based on your requirement for notification. Select the appropriate Priority.
- **Assign owner** ?
- **Check for every** ?

Alert Profile Examples

With the combinational usage of Alert Profile Type, Filters, and Threshold parameters, you will be able to create Alert Profiles addressing your precise and selective needs. Some of the example profile are discussed below:

- Say, you want to get notification of all Critical Events, enter the criteria as **Severity** is '2'. For the severity and severity number mapping refer the table given below.
- Same way, if you want to get notification of all attack logs, enter the criteria as **RecordType** is 'attack'.
- If you want to get notification for all virus logs, enter the criteria as **RecordType** is 'virus'.

The mapping table of severity number and severity

Severity	Severity Number
Emergency	0
Alert	1
Critical	2
Error	3
Warning	4
Notification	5
Information	6

Viewing Alerts

After setting up an Alert Profile, select the **Alerts** tab to see the list of alerts triggered. By default, the Alerts tab lists all the alerts triggered so far. The list shows the timestamp of the alert, the host which triggered it, the alert priority, and the status of the alert. Clicking on each alert profile would provide the details of the alert like why, when, & for which device the alert was triggered.



Viewing Alerts for an Alert Profile



The Alerts box on the left navigation pane lists all the alert profiles created so far. Click on each alert profile to view the corresponding list of alerts triggered.

The  icon against an alert profile indicates that an email notification has been setup.

The  icon against an alert profile indicates that a **Run Script** action has been setup.

The  icon against an alert profile indicates that an SMS notification has been setup.

The  icon indicates that the alert profile is currently enabled and active. To disable the alert profile, click on this icon. The alert profile is now disabled, and the  icon is shown. When an alert profile is disabled, alerts will not be triggered for that alert profile. To start triggering alerts again, click on the icon to enable the alert profile.

To **edit an alert profile** click on  icon. To **delete an alert profile**, click on the  icon.

The **Alerts** tab lets you view alerts for various alert profiles set up. To manage alert profiles, click the **Alert Profiles** link in the **Settings** tab.

Alerts Administration

Select the **Alerts** tab to see the list of alerts triggered. By default, the Alerts tab lists all the alerts triggered so far. The triggered alerts can be administered by the users of Firewall Analyzer application.

This topic explains the following sub-topics of alert administration.

- All Alerts
- Administering Alerts
- Alert Actions
- My Alerts

The administrator or operator can keep track of the actions taken on a particular alert. The actions are:

- The user can add a note or view the note(s) added by other users.
- The users can view the complete history of actions and notes on the alert but will not be able to modify the contents.
- The administrator can assign an alert to operator user.
- The operator can assign the alert to another operator user.
- The assigned user can remediate the alert and add the notes.
- The administrator only can delete the alerts which are not required any longer.

The **All Alerts** list shows the following:

Alert Profile	- the alert profile which triggered the alert.
Generated Time	- the time stamp of the alert.
Device	- the host which triggered the alert.
Priority	- the alert priority (high, medium, low) which was set as per requirement at the alert profile creation time.
Status	- the status of the alert notification, if any notification is configured.
Alert Owner	- the Firewall Analyzer application user assigned as owner to remediate the triggered alert
Action	- the action by the user on the alert, to add or view notes on the alert and delete the alert.

Administering Alerts

Clicking on each alert profile would display the details of the alert and the details of the alert profile which triggered the alert.

The **Alert Details** are:

Criticality	- the alert priority (high, medium, low) which was set as per requirement at the alert profile creation time the host which triggered the alert.
Last Event Message	- the last event (type) message, which triggered the alert notification.
Alert Profile Name	- the name of the alert profile which triggered this alert. Besides the name, there is a link named " View all the alerts generated by this profile ". Clicking the link displays all the alerts generated by the profile.
Alert Notification Status	- the status of the alert notification, if any notification is configured.
Date & Time	- the time stamp of the alert.
Alert Actions	- the action by the user on the alert, to add or view notes on the alert, assign owner, view alert history, and delete the alert.

The **Alert Profile Details** are:

Matching Conditions	- the matching condition(s) set in the alert profile to triggered an alert.
Latest Record	- displays the record of the last event, which triggered the alert notification.

Alert Actions

The actions which can be performed by the users are:

Add/View Note	- the user can add a note or view the already existing note entries pertaining to this alert. Any user can add a note to the alert.
Assign Owner	- any user, higher in the hierarchy can assign an user, lower in the hierarchy, as owner to the alert to remediate. The hierarchy of users in the Firewall Analyzer application is: <i>Admin > Operator > Guest</i> . The lower hierarchy users can assign the alert to the user of same hierarchy, but cannot assign to the user in higher hierarchy.
Alert History	- all the actions like creation, assigning owner along with the notes, if any will be listed for the particular alert.
Delete Alert	- the administrator user can only delete the alert if it is not required any longer.

My Alerts

My Alerts lists the alerts assigned to an operator user either by another operator user or admin user. Same way, it lists the alerts assigned to an admin user either by another admin user or himself. It is displayed below the All Alerts on the Left Navigation Pane, only if alerts were assigned to the logged-in user. The **My Alerts** list displays the alert details same as that of the **All Alerts** list.

System Settings

Configuring System Settings

The **Settings** tab lets you configure several system settings for the server running Firewall Analyzer, as well as other settings.

The **Simulate** option sends sample firewall logs to Firewall Analyzer so that you can view reports without having to send actual firewall logs. At any time, click the **Stop Simulate** link to stop sending sample data.

The **Data Storage Size** section in the left navigation pane of **Settings** tab lets you to configure data storage duration settings for the database and archive of Firewall Analyzer

The following is the the list of configuration options available under the System Settings section:

Setting	Description
Syslog Server Settings	Click this link to configure syslog servers to receive logs at different ports
Checkpoint Firewall Settings	Click this link to configure settings specific to CheckPoint firewalls
Alert Profiles	Click this link to view the alert profiles set up so far
Configure DNS	To configure resolving of DNS reverse lookup, globally for all the reports.
User-IP Mapping Configuration	To map the users with the IP address using DHCP or proxy logs.
Import Log Files	Click this link to import log files from the local machine or by FTP
Device Details	Click this link to view details of logs received from each device
Archived Files	Click this link to configure archiving intervals, or load an archived file into the database
Device Rule	To configure viewing of Used and Unused rules of a Firewall device.
Diagnose Firewall Connections	To monitor and analyze live connections through the Firewall
Schedule Listing	Click this link to view the list of reports scheduled
Working Hour	Click this link to configure Working and Non-Working hour firewall event log collection pattern of the organization.
Customize Report	To customize the device specific reports to be shown in Device Tree and the Reports page.
Rebranding FWA Web Client	To customize Firewall Analyzer Web Client to suit the needs of Managed Security Service Providers (MSSPs) or large enterprises

The following is the the list of configuration options available under the Administration Settings section:

Setting	Description
Protocol Groups	Click this link to manage protocol groups
Intranet Settings	Click this link to configure intranets to identify internal and external traffic
User Management	Click this link to add, edit, or delete users in Firewall Analyzer

Setting	Description
External Authentication Settings	Click this link to configure Active Directory and RADIUS server authentication
Mail Server Settings	Click this link to configure the mail server
Firewall Availability Alert	Click this link to configure to trigger alerts if there was no logs from Firewalls for a specific period of time
Server Diagnostics	Click this link to view system-related information for Firewall Analyzer
Database Console	Click this link to access the database and execute queries
License Management	Click this link to manage the device licenses effectively
SMS Settings	Click this link to configure the alert notification by SMS messages

Simulating Firewall Logs

The **Simulate** option lets you test Firewall Analyzer with sample data before setting it up on your network. The sample data is taken from the **firewall_records.xml** file present in the `<FirewallAnalyzer_Home>/server/default/conf` directory on the server.



The **Simulate** option lets you view reports for firewalls only, and not squid proxy servers.

When you click the **Simulate** link from the welcome screen or the **Settings** tab, the syslog server in Firewall Analyzer starts receiving the sample data as logs. The server then analyzes this data and generates reports assuming this data to be actual firewall logs. As a result, you can view all the pre-defined firewall reports, create custom report profiles, and set up notifications just like you would when actual data is received.

At any time, click the **Stop Simulate** link from the **Settings** tab to stop sending the sample data to the server. However, data already sent to the server will be present until the database is reinitialized.

Configuring Data Storage Duration

Firewall Analyzer retains the Firewall log data in the database as well as archives the logs received from each Firewall device, and zips them in regular intervals. The **Archived Files** page displays files that have been archived for each device. Perpetual retention of data in the database as well as archives use a lot disk space. If you are concerned about the disk space used by Firewall Analyzer, use these options as per your policies. To provide you more control, Firewall Analyzer gives you options to configure the data retention period for the database and archiving separately.

Configuring the Retention Time Period

Select the **Settings** tab in the Web Client. On the left side of the screen, you will see **Data Storage Options** section below the **Settings** section.

In that section, there will be two configurations. One is **Database** and the other is **Log Archive**.

Database

In the **Database**, you can configure the time period to retain the Firewall log data in the database. The time period options are listed in the combo box.

The options are:

- 1 Year
- 6 Months
- 3 Months
- 2 Months
- 1 Month
- 1 Week
- 1 Day

Select the time period as per your requirement.

Log Archive

In the **Log Archive** you can configure the time period to retain the archived Firewall log data. The time period options are listed in the combo box.

The options are:

- 1 Year
- 6 Months
- 3 Months
- 2 Months
- 1 Month
- 1 Week

Select the time period as per your requirement.

Click the **Update** button to configure the data retention time periods.

The data retention configurations available are described below:

Configuration	Default Value
Database	1 Year
Log Archive	1 Year

The time period options are described below:




Time period	Description
1 Year	The log data will be retained for a period of 1 year and will be purged (from database/archive) after the time period.
6 Months	The log data will be retained for a period of 6 months and will be purged (from database/archive) after the time period.
3 Months	The log data will be retained for a period of 3 months and will be purged (from database/archive) after the time period.
2 Months	The log data will be retained for a period of 2 months and will be purged (from database/archive) after the time period.
1 Month	The log data will be retained for a period of 1 month and will be purged (from database/archive) after the time period.
1 Week	The log data will be retained for a period of 1 week and will be purged (from database/archive) after the time period.

To cater for auditing requirements, the archived data needs to be retained for 6 months to 1 year.

Managing Syslog Servers

The **Syslog Server Settings** page lets you manage the various virtual syslog servers set up to receive exported logs at different ports.

The default listener ports for the syslog server in Firewall Analyzer are **514** and **1514**. If your firewalls are exporting log files to either of these ports, you do not have to set up any virtual syslog servers.

The **Syslog Servers** table shows the various virtual syslog servers set up so far, along with their IP address, listener port, and status. You can delete a virtual syslog server by clicking the  icon. Once a virtual syslog server is deleted, the corresponding listener port is also freed. You can also stop the syslog collection by clicking the  icon and restart the syslog collection by clicking on the  icon.

Adding a New Syslog Server

The **Add Syslog Server** box lets you add a new virtual syslog server and begin listening on a new port for exported log files.

Enter a unique **SysLog Server Name** for the new virtual syslog server, and the listener port. The **Host Name/IP Address** field is currently not editable, and takes the IP address of the machine on which the Firewall Analyzer server is running.

Click **Add Syslog Server** to add this virtual syslog server, and begin listening for log files at the specified port.

Managing LEA Servers

The **CheckPoint Firewall Settings** link lets you manage the LEA servers (CheckPoint Management Servers) that have been configured to connect to Check Point firewalls and access the log files.

The list of LEA servers (CheckPoint Management Servers) configured, along with the respective LEA listener port and authentication details, is displayed. The details of the CheckPoint Firewalls are listed in a table. The description of the table columns are as given below:

Parameter	Description
Firewall Name	The name of the CheckPoint Firewall being monitored.
SysLog Server	The name of the SysLog server from which the log will be extracted.
Lea Port	The port on which Firewall Analyzer has to connect to the Check Point firewall for LEA (Log Extraction API) access.
Authenticated	Indicates whether the connection between Firewall Analyzer and CheckPoint Firewall is authenticated.
Remove	To remove the CheckPoint Firewall in Firewall Analyzer from being monitored.

Adding an LEA Server

Carry out the following procedure to add a CheckPoint Firewall in the Firewall Analyzer:

- Enter the host name of the LEA server (CheckPoint Management Servers)
- Enter the port on which it has to connect to the Check Point firewall.
- Use the **Enable Debugging Mode** checkbox to enable the CheckPoint firewall in debugging mode. For debugging the procedure is given below.
- If you are using an unauthenticated connection, select the **Use Un-Authenticated Login** radio button. Follow the detailed instructions to configure Check Point firewall in Un-Authenticated mode.
- If you are using an authenticated connection, select the **Use Authenticated Login** radio button. Follow the detailed instructions to configure Check Point firewall in Authenticated mode.
- Click **Save** to add the LEA server.

If you are unable to view the CheckPoint Firewall reports carry out the following procedure:

- Click the Edit/Delete icon of the firewall for which you are unable to view reports. Click **Save**.
- Click the **Enable Debugging Mode** checkbox to enable the CheckPoint firewall in debugging mode.

- Once saved, create a support information file through Support tab, and send to fwanalyzer-support@manageengine.com





The Configuring Check Point Firewalls section includes detailed instructions on configuring Check Point firewalls for reporting in Firewall Analyzer


Managing Alert Profiles





The **Alert Profiles** link lets you manage all the alert profiles set up so far.

- The **Add Alert Profile** link lets you create a new alert profile.
- The **Export Alert Profile** link lets you to export the existing alert profiles to use it afterwards.
- The **Import Alert Profile** link lets you to import the alert profiles saved using Export Alert Profile.

The Alert Profiles table lists the following details of all the existing alert profiles:

Columns	Description
Edit	Option to edit the alert profile
Profile Name	Name of the alert profile
Criticality	Criticality of the alert triggered by the profile
Action	Action to be initiated when an alert triggered by the profile
# Alerts	Number of times each alert has been triggered. Clear Generated Alerts - All the alerts generated by this profile can be cleared. Hover the mouse on the number of alerts and click the  Trash icon to delete all the generated alerts.
Alert Type	Denotes the type of notification
Mail-Id	Email address associated with the alert profile
Export As	Export all the alerts, triggered by the particular profile, in PDF format. Click the  PDF icon.

Click an alert profile to see the corresponding list of alerts triggered. The  toggle icon lets you enable or disable an alert profile and correspondingly start or stop triggering alerts for the same.

The  icon lets you edit an alert profile. The  icon lets you delete an alert profile. Once deleted, the alerts associated with this profile are also deleted from the database. The  icon indicates that an email notification has been set up for this alert profile. The corresponding email address is also displayed next to this icon. The  icon indicates that an SMS notification has been set up for this alert profile.

Export the existing alert profiles

Export Alert Profiles - Select the check boxes of alert profiles to be exported and click this menu. The profile will be downloaded as an XML file (**FirewallAnalyzer_Profiles.xml**), through your browser into your client machine.

Import alert profiles

Import Alert Profiles - Click this menu to import report profiles. On clicking the menu, **Select Alert Profiles file to import:** screen pops-up. In that, you will find **File Location** text box and **Browse** button besides. Enter the location of the XML file (**FirewallAnalyzer_Profiles.xml**) or use the browse button to locate the XML file. Click **Import** button to import the profiles in to Firewall Analyzer server and **Cancel** button to

cancel the import profiles operation. If the report already exist in Firewall Analyzer, clicking **Import** button will list **Failed To Import** option and the existing reports with check boxes and you will find **Over Write** button and **Cancel** button to cancel the import profiles operation. Select the check boxes of report profiles to overwrite and click **Over Write** button.



There will be no hosts configured for the imported alert profiles. You have to edit the report profile to configure the hosts.

Configuring DNS Resolution

Firewall Analyzer by **default** displays the IP addresses of the Source and Destination that participate in the conversation going through Firewall. It also has the option to resolve the IP addresses to DNS names (whichever could be resolved) in the individual reports. You can do it by clicking **Resolve DNS** link that is provided in the report page. Moreover, Firewall Analyzer provides an option to configure DNS resolution for all the reports.



DNS resolution can be configured by following the steps given below:

1. In the Firewall Analyzer web client, select the **Settings** tab.
2. In **Settings** screen, select the **System Settings > Configure DNS** link. **Resolve DNS Configuration** page appears.
3. On the top, there are three options provided with radio buttons. Select an option as per your requirement, by clicking the radio button. The options are:

- Do Reverse lookup automatically. I want to see DNS name everywhere instead of IPAddress.
- Don't do Reverse lookup automatically. Let me get an option to do that in my reports.
- No lookup at all. I want to see IPAddresses everywhere.

4. Select **IPAddress and DNSName mapping in memory** as per your requirement from the drop down list. The list options are 5000, 10000, and 20000. This denotes the number of IP address and DNS name mappings to cached in the memory of the machine. You can leave it undisturbed with the default value.
5. Click **Update** to effect the *Resolve DNS Configuration*. Click **Cancel** to cancel the configuration operation.

Manual DNS Configuration

If you want to configure DNS name manually, click the link "**Want to configure (Add/Edit) DNS name manually? Click Here**". **Manual DNS Configuration** page appears. Click the **Add Entry** link. This pops-up the **Manual DNS Addition** screen. In that screen, there will be two text boxes, "**Enter IP:**" to enter the IP Address and "**DNS Name:**" to enter the DNS Name to which the IP Address should be mapped. You can add more mappings using the **Add Entry** button at the bottom. Click **Update** to effect the *Manual IP,DNS Mapping* . Click **Cancel** to cancel the configuration operation. If you want to delete the manually added entries, select the checkboxes and click the '**Delete**'  icon. Click the '**Edit**'  icon to modify the entries.



- The '**Add Entry**' manual configuration will update IP, DNS mappings into Firewall Analyzer memory.
- Manually added values will overwrite already resolved IP,DNS mappings.
- On the fly report generation is possible, if you configure DNS mapping manually in case of dynamic IP address allocation using DHCP protocol.

Description of the options

- **Do Reverse lookup automatically. I want to see DNS name everywhere instead of IPAddress.**

In this option, Firewall Analyzer will perform reverse NS lookup of all IP addresses automatically. This will be carried out for all the reports and the only DNS names (whichever could be resolved) will be displayed in the reports.


Use this option, if you want to see only DNS names of the hosts in all your reports.

- **Don't Reverse lookup automatically. Let me get an option to do that in my reports.**

In this option, Firewall Analyzer will not perform reverse NS lookup of IP addresses automatically and will display the IP addresses of the Source and Destination that participate in the conversation going through Firewall and if you want DNS names to be displayed for the hosts for a particular report, you can use the **ResolveDNS** link in the report.

In each of the individual reports a **ResolveDNS** link has been provided at the top. Clicking this link enables DNS Resolution for all the IP Addresses of the unresolved hosts present in the current report. The status of DNS Resolution depends on the default DNS lookup time, within which Firewall Analyzer will try to resolve the IP Address.

This is an existing option. Use this option, if you want to see DNS names of the hosts only in particular reports.


	<p>If DNS Resolution is in progress for any other Firewall Analyzer user, then the subsequent user will see the message "<i>Please wait, DNS Resolution in progress for another user</i>" when clicking ResolveDNS link. Once the DNS Resolution is complete for the first user, then the DNS Resolution for the subsequent user begins automatically.</p>
---	--

- **No lookup at all. I want to see IPAddresses everywhere.**

In this option, Firewall Analyzer will display only the IP addresses of the Source and Destination that participate in the conversation going through Firewall.

If you select this option, **Resolve DNS** option will not be available for any of the reports.

Use this option, if you want to see only IP addresses of the hosts in all your reports.

	<p>Firewall Analyzer will resolve all the IP Addresses into DNS names which are resolved by the 'nslookup' command from the machine where the product is installed.</p>
---	--

Mapping User Name vs IP Address using DHCP/Proxy Logs

Firewall Analyzer by **default** displays the IP addresses of the Source and Destination that participate in the conversation going through Firewall. It provides you with an option to associate the IP addresses to User Name or MAC Address in the Firewall reports. The user name/Mac address to IP address can be mapped using DHCP or Proxy logs. You can do it by clicking **User-IP Mapping Configuration** link that is provided in the **Settings** page.

Carry out the procedure given below to configure the User Name - IP Address Mapping:

1. In the Firewall Analyzer web client, select the **Settings** tab.
2. In **Settings** screen, select the **System Settings > User-IP Mapping Configuration** link. **IP Address to User Mapping** page appears.
3. In the **Configuration Details** section, there are three options provided with radio buttons. Select an option as per your requirement, by clicking the radio button. The options are:


- **Get User Names from Proxy logs and associate with Firewall logs**
- **Get Host Name / MAC Address from DHCP logs and associate with Firewall logs**
- **None [Default]**

- a. **Get User Names from Proxy logs and associate with Firewall logs**

You can select this option to get User Name instead of IPAddress in all reports. Source & Destination IP Address of configured Firewalls will be replaced by User Name got from the Proxy Servers.

- Select the **Get User Names from Proxy logs and associate with Firewall logs** radio button to assign devices to a particular Proxy Server. Below the selected option, a table with proxy server and devices assigned to it, appears in the screen.

The details of the columns of the table are:

Proxy Server Details	Description
Proxy Server Name	The names of the proxy server from which the Firewall Analyzer will associate user name with the Firewall log data. In this case, all the Proxy servers added to the Firewall Analyzer will be listed.
Assigned Devices	The Firewall devices assigned to the particular proxy server.
Assign/Edit Devices	Click the icon to view the devices assigned to the proxy server and modify the devices assigned to the proxy server. If no device is assigned, you can assign devices to the proxy server.
Delete Assigned Devices	Delete the assigned devices to the proxy server for User-IP Mapping purpose. Click the  icon to delete the assigned devices.

- Click the **Assign/Edit Devices** icon to assign devices to the proxy server. The **Assign Devices** screen pops up.
 - Select the devices, which you want to assign/re-assign to the selected proxy server. All the available devices are listed in the **Available Device(s)** list. Select the devices and click right arrow. The selected devices are moved to the **Selected Device(s)** list. If you want to remove any device from the **Selected Device(s)** list, select the devices and click left arrow. The removed devices will be moved back to the **Available Device(s)** list.
- Click **Save** button to assign the selected devices to the selected proxy server. Click **Cancel** to cancel the assigning devices to the proxy server operation.

After associating the devices to proxy server the proxy server and the assigned devices are listed in the table.

b. **Get Host Name / MAC Address from DHCP logs and associate with Firewall logs**

You can select this option to get Host Name / MAC Address instead of IP Address in all reports. Source & Destination IP Address of configured Firewalls will be replaced by MAC Address got from the DHCP Servers.

- Select the **Get HostName / MACAddress from DHCP logs and associate with Firewall logs** option from User-IP Mapping Configuration page and

click **Save** button to save the settings. Below the selected option, you will find an option **Add DHCP Servers as separate device** with a check box. Select this option if you want to enable Raw Log Search over DHCP Logs.

- Import the DHCP logs.
 - Import DHCP logs if DHCP server is running in Windows.
 - Use Syslog daemon option available in your Linux box or Use Remote Import option with Periodic Interval.



Note: When you import the DHCP logs, ensure to configure that the DHCP logs are periodically imported from DHCP server.



Note: When you import the DHCP logs from DHCP server, ensure to select the 'Ignore UnParsed/Junk Record(s)' check box in the '**Import Log File**' screen. Refer the screen shots below for Local Host and Remote Host.

Local Host

Import Log File

Import Log file from the desired location

☒ Local Host

☐ Remote Host

Note : Log records imported from local host. Protocol: HTTP, Max File Size: 1 GB.

File Location : No file chosen

☒ Ignore UnParsed/Junk Record(s)

Remote Host

Import Log File

Import Log file from the desired location

☐ Local Host
 ☒ Remote Host

Note : Log records imported from remote host. Protocol: FTP, Max File Size: 2 GB.

Remote HostName/IP:

Remote Username:

Remote Password:

Time Interval (Min):

☒ Ignore UnParsed/Junk Record(s)

Location: [List Files/Directories](#)

☐ Change filename dynamically

- Go to User-IP Mapping Configuration page and associate the Firewalls to detected DHCP server. In that page, below the selected option, you will find a table with DHCP server and devices to be assigned or assigned to it.

The details of the columns of the table are given below:

DHCP Server Details	Description
DHCP Server Name	The names of the DHCP server from which the Firewall Analyzer will associate user name with the Firewall log data. <i>In this case, only after the Get HostName / MACAddress from DHCP logs and associate with Firewall logs option is selected and saved and import of DHCP server logs in to the Firewall Analyzer, the DHCP servers will be listed.</i>
Assigned Devices	The Firewall devices assigned to the particular DHCP server.
Assign/Edit Devices	Click the icon to view the devices assigned to the DHCP server and modify the devices assigned to the DHCP server. If no device is assigned, you can assign devices to the DHCP server.
Delete Assigned Devices	Delete the assigned devices to the DHCP server for User-IP Mapping purpose. Click the ✗ icon to delete the assigned devices.

- Click the **Assign/Edit Devices** icon to assign devices to the DHCP server. The **Assign Devices** screen pops up.
 - Select the devices, which you want to assign/re-assign to the selected DHCP server. All the available devices are listed in the **Available Device(s)** list. Select the devices and click right arrow. The selected devices are moved to the **Selected Device(s)** list. If you want to remove any device from the **Selected Device(s)** list, select the devices and click left arrow. The removed devices will be moved back to the **Available Device(s)** list. After associating the devices to DHCP server the proxy server and the assigned devices are listed in the table.
- Click **Save** button to assign the selected devices to the selected DHCP server. Click **Cancel** to cancel the assigning devices to the DHCP server operation.
- Click **Save** button in the User-IP Mapping Configuration page to save the settings again.

User name got from upcoming DHCP logs will be associated to the IP Addresses of upcoming associated firewall logs.

c. **None [Default]**

In this option, Firewall Analyzer creates the reports based on IP Address or DNS Name with respect to Resolve DNS Configuration Settings. Only the IP Addresses or the DNS Name of the Source and Destination that participate in the conversation going through Firewall will be displayed.

If you select this option, **User Name - IP Address Mapping** option will not be available for any of the reports. Select this option, if you want to see only IP Addresses or DNS Names of the hosts in all your reports.

4. Click **Save** to effect the *IP Address to User Mapping Configuration*. Click **Cancel** to cancel the configuration operation.

Importing Log Files

The **Import Log Files** link lets you import a log file from the local machine or remotely, through FTP. The **Imported Log Files** page shows you the list of log files imported, along with details such as the host from which it was imported, and the status of the import. Importing of archived files (.gz format) created by Firewall Analyzer and zipped log files (.zip format) are also supported.



Use this option to import log files from squid proxy servers.

Click the **✖** icon to delete an imported log file from the database.

Importing a Log File

1. Click the **Import Log File** link to import a new log file.
2. Choose **Local Host** if the log file is present in the local machine from which you are accessing the Firewall Analyzer server.
 - a. In the **File Location** text box, enter the location of the file or click **Browse** button to select the log file.
 - b. The option **Ignore UnParsed/Junk Record(s)** enables the Firewall Analyzer to skip those records in the imported log file, that are in unsupported format and continue with parsing the subsequent supported records in the file. If not selected, the Firewall Analyzer will not parse the entire log file even if one record contains unsupported log format.
 - c. The option '**Consider this as Virtual Firewall with IP Address _**' check box and text box enable the

Firewall Analyzer to identify the imported log file as the log file from a specific virtual Firewall (vdom). Select the check box and provide the appropriate Firewall physical IP address in the IP address text box. Otherwise the imported logs will be considered as logs of a physical Firewall device.

- d. Enter the **Time Interval** (Scheduling time in Minutes) after which Firewall Analyzer should retrieve new log files.
- e. Select the **Change filename dynamically** option, if you want to import the log files which change their names dynamically.
- f. Select the date and/or time file name pattern from the **Filename pattern**: combo box or add a new pattern using the Blue Cross icon.

Note: Schedule and Change filename dynamically options will appear only when the Firewall Analyzer client is invoked from the server machine itself.

3. Finally, click **Import** to import the log file into the database.
4. Choose **Remote Host** if you need to import the particular log file or the entire directory containing the log files from a remote location on the network.

- a. Enter the remote host's HostName or IP address in the **Remote HostName/IP** text box, and the FTP user name and password in the **Remote Username** and **Remote Password** text boxes.
- b. Enter the **Time Interval** (Scheduling time in Minutes) after which Firewall Analyzer should retrieve new log files.
- c. Select the **Ignore UnParsed/Junk Record(s)** option as per requirement.
- d. The option '**Consider this as Virtual Firewall with IP Address _**' check box and text box enable the

Firewall Analyzer to identify the imported log file as the log file from a specific virtual Firewall (vdom). Select the check box and provide the appropriate Firewall physical IP address in the IP address text box. Otherwise the imported logs will be considered as logs of a physical Firewall device.

- e. Enter the location on the remote machine where the log file or the entire directory containing the log files is present in the **Location** text box. You can click the **List Files/Directories** link to locate the file on the remote computer.
 - f. Select the **Change filename dynamically** option, if you want to import the log files which change their names dynamically.
 - g. Select the date and/or time file name pattern from the **Filename pattern:** combo box or add a new pattern using the Blue Cross icon.
5. Finally, click **Import** to import the log file into the database.

Local Host:

- Log records imported from local host. Protocol: HTTP, Max File Size: 1 GB. If the log records are imported from local server (where Firewall Analyzer is running), there is no maximum file size limit.
- Scheduled local import is supported in Firefox, Internet Explorer and Opera browsers
- To import log from another machine using localhost option, you can share the folder of the another machine and map that shared folder as network drive of localhost. You can schedule the log import for this also.
- Firefox browser users need to configure one-time settings. Follow the procedure given in the Firefox Settings section of local import page.



Remote Host:


- Log records imported from remote host. Protocol: FTP, Max File Size: 2 GB

Firefox Setting (This is a One-Time configuration)

- Open a new browser tab/window and enter '*about:config*' in the address bar
- Right click and select **New > Boolean**
- Enter '**signed.applets.codebase_principal_support**' as a new preference name and close the tab/window
- Import the log file again from the local machine. The browser asks for permission.

Enable '**Remember this decision**' and click '**Allow**'



	<ul style="list-style-type: none"> If you have selected the Ignore UnParsed/Junk Record(s) while importing the logs, the records will not be shown when the  icon is clicked on the sub tab. Microsoft ISA Proxy creates log file with new name (with time stamp appended) everyday. If the Microsoft ISA Proxy log files are to be imported, you do not have to change the filename daily, instead select the Change filename dynamically option while importing the logs. Selecting the option displays the the Filename pattern: text box to enter the time stamp pattern that the Proxy server appends when the Proxy server creates the log file daily. A help tip icon displays, (when you hover the mouse on the icon) the mapping of the <i>Timestamp in Filename</i> to the <i>Pattern to be given</i>. Enter the pattern as required.
---	--

The supported formats for imported log files is shown below the **Location** box. We also support importing of archived files (.gz format) created by our Firewall Analyzer. If you are importing an unsupported log file, a warning message is shown. You can still import the file, but records will show up when the  icon is clicked on the sub tab.

The time taken to import a log file depends on its file size. Once the file has been imported successfully, the device from which it was imported is listed in the appropriate category, and the reports are generated automatically.

The **Imported Log Files** table shows the list of all log files imported so far. In this list, the latest imported log file will appear on the top.

The list contains the following columns:

Column Head	Description
File Name	Name of the imported log file. Click on the  icon to know the details of errors while importing the log files.
Remote Host	Remote Host from where the log file has been imported.
Protocol	HTTP for local host and FTP for remote host.
Status	Indicates the status of file import. Various status are listed below.
Imported Time	The time stamp at which the log file was imported.
Size	The size of the imported log file.
Time Taken	The time taken to import the log file.
View Report	This column will display a View Report link, if report for the imported can be generated. On clicking the link, it will redirect to the dashboard.
Action	No action for log files imported from local hosts and enable or disable collecting logs from the device (using  toggle icon) at specific time interval for remote hosts.

The number of imported log files listed per page can be selected in **View per page:** list (5, 10, 20, 50, 100). *HTTP* is displayed in the **Protocol** column, if logs have been imported from the local machine. *FTP* is displayed in the **Protocol** column, if logs have been imported from a remote machine. Click the *FTP* link to see the remote host details and file details for the log file imported. Click the ⚡ toggle icon in the **Action** column to enable or disable collecting logs from this device after the specified time interval. Select the check box(es) of imported log file(s) to be deleted (there is a separate check box for each imported file) and click the ✖ icon to delete all log files imported from this device.

Status of File Import

- Received log file for import
- The file has not been modified, since last update
- Continuing to parse log file from last update...
- File received, loading the file into DB
- Batch processing started...
- Generating reports...
- Import of log file completed
- Import of log file failed!
- Import task enabled!
- Import task disabled!
- Import task already disabled!
- Import task already enabled!
- Import task not available!
- Processing request

Viewing Device Details

The **Device Details** link shows you the various devices from which logs are collected in Firewall Analyzer.

The **Supported Logs Received** table shows all the devices from which logs supported by Firewall Analyzer, are received. The table lists the device details like Device Name, Device Type (Firewall, Squid, etc.), timestamp of the last received log file, the syslog port, current status of log collection, Action (Edit, Delete) and the Manage Status (Managed, Unmanaged).

In the **Actions** column, click on the  **Edit** icon next to a device to change the device name or the link speed values. Click the  **Delete** icon to delete the device from the database. All logs collected from that device will also be deleted.

Clicking **Edit** button pops-up, **Edit Firewall Property** screen. The screen displays **Firewall Name**, **Firewall IP**, **Display Name**, **Vendor Type**, **Down Link Speed (in Kbps)**, and **Up Link Speed (in Kbps)**. You can configure the **Display Name**, **Down Link Speed (in Kbps)**, and **Up Link Speed (in Kbps)** of the device. If the Firewall Analyzer is able to query the Interface Up Link and Down Link Speeds of the device using SNMP, the same will be displayed here. However you can edit as per your requirement. If the Firewall Analyzer is unable to query the Link Speeds, enter it manually in this screen. Link Speed is used to calculate the percentage utilization in Live Reports. Click **Update** button to update the device configuration and **Cancel** button to cancel the operation.

The **Unsupported Log Record Details** table shows all the devices from which logs that are not supported by Firewall Analyzer are received.

Click the **View Record** link to view the first few lines from the unsupported log record. Click the **Tell Us** link to open a popup window, through which you can send a mail to the Firewall Analyzer Technical Support team telling us about the unsupported log format. Type the relevant details, and click **Send Mail** to send the message. The Technical Support team will get back to you with more details about the unsupported log format, and how we can help you.

The **Schedules Executed** table shows the schedules that have run so far, along with the user that executed the schedule, the report profile the schedule was associated with, and the status of execution of the schedule.

Archiving Log Files

Firewall Analyzer archives the logs received from each device, and zips them in regular intervals. The **Archived Files** page files that have been archived for each device, along with options to load the file to search, and delete the file.

Encrypting Archived Log files

Firewall Analyzer encrypts the log archive files to ensure the log data is secured for future forensic analysis and internal audits. Encryption makes the log data unreadable for human. It can be only decrypted by the Firewall Analyzer application.


Time stamping

The time stamping technique ensures that the archive data files are tamper proof. If there is a modification of file, this technique will reveal that the file has been tampered.

Loading Archived Files

The **Archived Files** page lists the files that have been zipped for each device, along with the archived time, file size, and archiving status.

The list contains the following columns:

Attribute	Description
Device	The name of the device for which the log file is archived.
File Name	
Start Time	The starting time of the log file archiving process.
Archived Time	The completion time of the log file archiving process.
File Size	The file size of the archived logs.
Status	You can view the log file archiving status in this column. The status values are: <i>All, Loaded, Loading, Not Loaded, Verified</i> and <i>Tampered</i> . The appropriate status value will be displayed, denoting the file archiving status. While loading Archived Files, if the archived file is tampered, it will not be loaded and marked as Tampered . If it is not tampered, it will be marked as Verified .
Action	You can carry out the following actions on the archived log files. The Actions are:  Load to Search and Report . The Actions are discussed below.


To load an archived file for search, click the **Load to Search** link against the device for which you need to see archived data. Once the file is fully loaded, you can search for data in the archives, and view specific information.

If you click **Load to Search** link, the **Raw Log Search** screen pops up. In the screen, on top you will find **Device Name** : <>, **Defined Criteria** : -, **Searched From** : *Traffic Logs*


You will find **Edit Search Criteria** link to edit and modify the search criteria.

On clicking the link, you will find **Device Name** *pix501(non-editable)*, **Search Time From:** <> **To:** <>. Next there will be two tabs: **Search Traffic Logs** and **Search Security Logs**. Choose one of the tabs as required. Define the search criteria in the **Define Criteria** section using the options **Match all of the following**, **Match any of the following**, select criteria and logical operator from the from the list and enter the value in the text box. Use **Add Criteria** and **Remove Criteria** links to add more than one criterion. The search criteria for Security logs are: *Protocol, Source, Destination, User, Virus, Attack, Severity, URL, Status, Rule, VPN, Duration, Message*. The search criteria for Traffic logs are: *Protocol, Source, Destination, User, Sent (in Bytes), Received (in Bytes), Rule, VPN*.

Then, you can view the raw logs **Search Result Between [YYYY-MM-DD HH:MM:SS to YYYY-MM-DD HH:MM:SS]**. You can click **View All Security Logs** link to view all the security logs.

Below that, you will find **Formatted Logs**, **Raw Logs** tabs. You can choose the tabs to view either formatted logs or raw logs. Click  **Configure Columns** to select the columns to be displayed for the formatted logs. The columns are: *All Columns, Device, Host, User, Protocol, Destination, Date/Time, Virus/Attack, VPN, Severity, Rule Number/ID, Status, URL, Duration, Description, StartTime*. You can export the search result as report in PDF or CSV format using **Export as: PDF, CSV** link.

Below that, the number of lines of logs displayed are indicated in the **Showing : _ to _ of total _ logs** field. The number lines displayed per page is indicated in the **View per page : 5 [10] 20 25 50 75 100 250 500** field. Default value is *10*. The default columns displayed are: *Host, Protocol, Destination, Date/Time, Status, Severity, and Description*. You can add or remove columns using **Configure Columns** icon given above.

Click the  icon against an archived file to delete it.




Once deleted, the archived data cannot be retrieved.

Viewing Data from Archived Files

Once the archive is fully loaded, click the **Report** link to search for specific data in the archive. In the popup window that opens, enter the criteria for the data, such as the firewall, user name, protocol, etc. You can enter a maximum of three criteria.

Choose the time interval for which you want to see the data that meets all the criteria. Click **Generate Report** to view the records that match the criteria that you have specified.

Changing Archive Settings

Click the  **Archive Settings** link to change the archiving intervals or to disable archiving. In the **File Archive Settings** popup window, uncheck the **Enable Raw Logs Archiving** check box to disable file archiving.

Log files are archived at specific interval configured in this screen.

The archiving options available are described below:

Attribute	Default Value	Description
File Creation Interval	12 hours	The time interval after which a log file is created for each host from which event logs are collected.
Zip Compression Interval	24 hours	The time interval after which log files created for each host are zipped to save disk space.
Start Initial Compression at	_ Hrs _ Mins	The time at which log files created for each host are zipped for the first time to save disk space.
Retain logs for	Forever	You can retain the archive log data as per the compliance audit requirement or internal audit policy requirement. The options available are: <i>Forever, 1 Year, 6 Months, 3 Months, 1 Month</i> and <i>1 Week</i> . Select the option that suits your requirement.
Archive File Encryption	Disable	Firewall Analyzer comes with a feature to encrypt the archive data. To enable encryption of archive data, select the Enable radio button and to disable, select Disable radio button.
Time Stamping	Disable	Firewall Analyzer comes with a feature to timestamp the archive data. To enable time stamping of archive data, select the Enable radio button and to disable, select Disable radio button.
Change Raw Logs Archive Location	<Firewall Analyzer Home>\server\default\archive directory	By default the Archive Location for the event logs and syslogs in Firewall Analyzer is <Firewall Analyzer Home>\server\default\archive directory, you can change this location by clicking the Edit link and providing the location as per your requirement.
Change Raw Logs Indexing Location	<Firewall Analyzer Home>\server\default\indexes directory	By default the Index Location for the event logs and syslogs in Firewall Analyzer is <Firewall Analyzer Home>\server\default\indexes directory, you can change this location by clicking the Edit link and providing the location as per your requirement.

You can create instant zip file of the existing log files waiting to be archived. Click **Zip Now** to create a zipped file with the currently available log files.






Click **Save** to save the archiving options, if you have changed them. Click **Close** to close the Archive Settings box.

Note: The currently active log files (i.e., logs not yet archived) will be stored in the <Firewall Analyzer Home>\server\default\archive\localhost\hot directory. The archived log files (i.e., logs archived as according to the archive settings) will be stored in the <Firewall Analyzer Home>\server\default\archive\localhost\cold directory. The archived log files loaded into database for analysis will be stored in the Warm directory. The log files will be stored in the <Firewall Analyzer Home>\server\default\archive\localhost\warm directory for 1 day and after that the log files will be purged.

Configuring to Fetch Firewall Configuration and Unused Rules

In a Firewall device, there could be numerous rules/access-list defined to secure the network from external attacks. Out of the rules/access-list configured, there could be certain rules which would be most used and certain which are least used or never used. Firewall Analyzer captures the most used rules in the **Top Used Rules** as they would be available in the logs generated by Firewall. But, to get the **Unused Rules**, one needs to configure the Firewall Analyzer to fetch the complete rules from the device. Once, Firewall Analyzer fetches the complete rules configured in the Firewall, it can provide the **Unused Rules** view.


To view Unused Firewall Rules, configure the Firewall Analyzer by following the steps given below:

1. In the Firewall Analyzer web client, select the **Settings** tab.
2. In **Settings** screen, select the **System Settings > Device Rule** link. **Device Rule Info** page appears.
3. On the top, there are links provided to add device info to fetch rules and to delete the device info. The links are:
 - a.  Device Info
 - b.  Device Info
 - c.  Profile
 - d.  Assign Profile
 - e.  List Profile
 - f. Change Management Configurations

Add Device Info

4. Click the **Add Device Info** link to add the device information to fetch the rules and configurations using Telnet or SSH. The **Enter Device Details** screen opens up.
5. In the **Enter Device Details** screen, select the Firewall device in the **Select Device** drop down list.
6. In the **Fetch Rules/Config** section, there will be two options to fetch rules and configurations
 - a. **From Device**
 - b. **From File**

Select the option as per your requirement.

	<p>Fetching the rules directly from the device is supported for the following devices only:</p> <ul style="list-style-type: none"> • Cisco • Fortigate • Netscreen <p>For the rest of the devices, please use the Fetch Rules/Config > From File option.</p>
---	---

Fetch Rules/Config > From Device

You can configure the individual device credentials to fetch the rules and configuration from the device or you can create a common profile of device credential which can be used for a group of devices to fetch rules.

7. In the **From Device** tab, select the protocol (Telnet or SSH) in the **Protocol** drop down list.
8. In the **Use Profile** tab, select the profile in the **Use Profile** drop down list. If there is no profile available or you want to create and use a new profile, click **New Profile** link besides the combo box.
9. Enter the Device Info. The Device Info has been split into two sections:
 - **Primary Info** - deal with parameters that are necessary to establish communication with the device. Details such as Login Name, Password, Prompt, Enable UserName, Enable Password and Enable Prompt are classified as basic details.
 - **Secondary Info** - certain parameters usually take standard values. All such parameters have been classified under 'Secondary Info'. Port, login prompt, enable user prompt, password prompt, enable password prompt values are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

Primary Info

Device Info	Description
Login Name	While establishing connection with a device, if the device asks for a Login Name, set a value for this parameter. This parameter is Optional.
Password	To set the Password for accessing the device.
Prompt	The prompt that appears after successful login.
Enable UserName	When entering into privileged mode, some devices require UserName to be entered. Provide the username if prompted; otherwise leave this field empty.
Enable Password	This is for entering into privileged mode to perform configuration operations like backup/upload. This parameter is mandatory.
Enable Prompt	This is the prompt that will appear after going into enable mode.




Both Primary and Secondary credentials (Login Name and Password) of the Firewalls are encrypted and stored in the Firewall Analyzer.

Secondary Info

Click the link **Secondary Info** to view/enter values for these parameters. All the parameters are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

Device Info	Description
IP Address	IP Address of the Firewall device to which the Firewall Analyzer will connect through FTP. See Note below.
Port (Telnet/SSH)	Port number of Telnet/SSH - 23 (for Telnet) and 22 (for SSH) by default.
Login Prompt	The text/symbol that appears on the console to get the typed login name is referred as login prompt. For example, Login:
Password Prompt	The text displayed on the console when asking for password. For example, Password:
Enable User Prompt	The text displayed on the console when asking for Enable UserName. For example, UserName:
Enable Password Prompt	The text displayed on the console when asking for password. For example, Password:

10. The command to be executed, to fetch the Firewall rules is displayed in the **Command** field.
11. Select **Fetch Rules from the device** check box to fetch the rules from the Firewall device.
If commands are not available to fetch rules from the device, **Choose File** button automatically appears besides the select item. If the file is not yet selected, '**No file chosen**' message appears besides the button. If it is not supported for the particular device [**Not Supported**] messages appears besides the select item.
12. Select **Generate Compliance Report** check box to generate Firewall Compliance report. If commands are not available to fetch configurations from the device, **Choose File** button automatically appears besides the select item. If the file is not yet selected, '**No file chosen**' message appears besides the button. If it is not supported for the particular device [**Not Supported**] messages appears besides the select item.



In the Fetch Rules from the device section, if the following message appears: '**Unable to generate compliance report. Reason: Failed to locate Nipper. Click here to enable it**'. Carry out the procedure given at the end of the document.

13. Select **Generate Change Management Report** check box to generate configuration change management report. When you select this report option, **Notification Options** and **Scheduling Options**, for the configuration changes of the device, will appear. If commands are not available to fetch configurations from the device, there will not be any Change Management report.
14. Under the **Notification Options**, enter the Email address of the user(s), who need to be informed via Email when any configuration change happens, in the **Mail To:** text box. Click the link **Click here to configure** to configure mail server for Firewall Analyzer.
15. Under the **Notification Options**, enter the cellular phone number of the user(s), who need to be informed via SMS when any configuration change happens, in the **SMS To:** text box. Click the link **Click here to configure** to configure SMS server for Firewall Analyzer.
16. Under the **Scheduling Options**, enter the Email address of the user(s), to whom the report to be sent via email when a scheduled configuration change report is generated, in the **Mail To:** text box. Click the link **Click here to configure** to

configure mail server for Firewall Analyzer. Select the schedule for report generation using the **Get Report for Every <1 to 31> day(s) @ <0 to 23> Hrs <0 to 50> Min.** (For example: If you configure like **Every 10 day(s) @ 2 Hrs 30 Min**, the reports will be generated for the device, every 10 days at 02:30 AM), **For the <Previous Week, Last 7 Days, Previous Month, Last 30 Days>** for the selected duration. Select the report format to be sent via email using the **PDF, CSV** radio buttons.

17. Select the **Yes** or **No** radio button of **Periodic rule/configuration fetching** option to fetch the rules/configurations periodically or once.
 - a. Select **Yes** radio button to fetch the rules/configurations periodically. The periodicity option opens up. Select the periodicity of rules fetching from the combo boxes given in: **Every <1 to 31> day(s) @ <0 to 23> Hrs <0 to 50> Min.** (For example: If you configure like **Every 10 day(s) @ 2 Hrs 30 Min**, the rules will be fetched from the device, every 10 days at 02:30 AM)
 - b. Select **No** radio button to fetch the rules/configurations once.
18. Click **Test Now** button, to test the validity of the device info; otherwise, click **Save** button to apply the values. Click **Cancel** to cancel the adding device info operation.



If the Firewall Analyzer is not receiving the logs directly from the Firewall device (i.e., the logs are received from a log forwarder tool), to fetch the rules from the Firewall device, configure the IP Address of the actual Firewall. Configure the IP Address, using **Secondary Info > IP Address** field.



Generating Change Management Report is supported for the following devices:

- Cisco
- Fortigate
- Netscreen
- Juniper SRX




Getting Rules/ Configuration Information from the individual virtual Firewalls (vdom/context)

- **Add Device Info** menu supports fetching the rules/configurations for the Firewall devices. It lists only the physical devices in the **Select Device** drop down list. It does not distinguish between vdom/context enabled Firewall and normal Firewall device. By default, both the vdom/context Firewall (if any) and the physical Firewall rules and configurations are fetched.
- If you want to fetch the rules/configurations for a selected vdom/context individually, create a separate Device Profile and associate the vdom/context to the profile for which you need the reports. Select the option '*Display Virtual Domains in the below resources list.*' in **Associate Profiles to Devices** page. It lists both the virtual Firewalls (vdom/context) and the physical Firewall devices in the **Select Device** drop down list.

Fetch Rules > From File

12. In the **From File** tab, you will find the two options: **Import Rule File** and **Import Configuration File**.
13. In the **Import Rule File** option, click the **Browse** button to locate the file which contains the rules details of the Firewall device.
14. In the **Import Configuration File** option, click the **Browse** button to locate the file which contains the complete configuration details of the Firewall device.
15. Click **Import** button to import the rule/configuration file. Click **Cancel** to cancel the rules/configuration details file importing operation.

For the complete procedure to export the configuration from various Firewalls in file format, refer the Exporting Configuration Files page.

	<p>Rule File</p> <ul style="list-style-type: none"> • User should create a rule file containing rules details. • The file should contain rule name, rule hash value (optional) and description only in comma separated format. • Each rule should be in a new line. <p>Configuration File</p> <ul style="list-style-type: none"> • Configuration File should contain complete configuration of device in readable format. <p> Only for Check Point Firewall</p> <ul style="list-style-type: none"> • In the case of Check Point firewalls, there will be multiple configuration files. In that case, if you are using "From File" mode, it should be provided in the Zip file format. • The configuration files are: <ul style="list-style-type: none"> ○ objects.C ○ objects.C_41 ○ objects_5_0.C ○ rules.C ○ rulebases.fws ○ rulebases_5_0.fws • The files are stored in the directory <i>conf</i> or <i>database</i>.
--	---

Delete Device Info

- To delete the Device Info from the list of Device Details table, select the check boxes of the respective Device Info entries and click the **Delete Device Info** link.

Testing the validity of device info

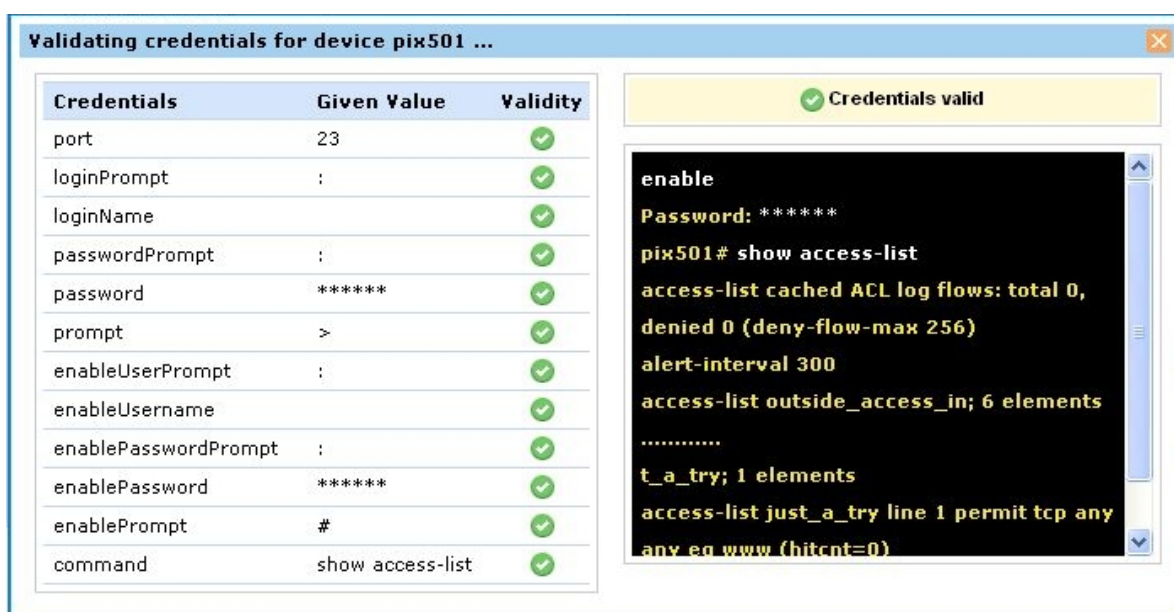
Device Info values entered through the Firewall Analyzer GUI should be accurate. Otherwise, Firewall Analyzer will not be able to establish connection with the device. To

ensure the correctness of device info values, Firewall Analyzer provides the testing option. After entering the device info, you can test the values during which Firewall Analyzer will indicate if the values entered are valid. It will pinpoint the invalid values and you can carry out corrections accordingly.

To test the validity of device info, follow the procedure given below:

- After providing the device info, click **Test Now** button.

This updates the device info values in the database and then carries out the testing. The result of the testing will be shown in a separate window as below:



The testing result indicates valid device info values with a green 'tick' mark. The invalid values are marked as red cross marks. You need to change the invalid values. Alongside, the CLI command execution result (through which Firewall Analyzer ascertains the validity of device info values) is also displayed.

List Device Info

Devices Details
















After entering and saving the Device Info values through the Firewall Analyzer GUI, the device, with details to fetch rules, is listed in the **Device Details** table. The details of the columns of the **Device Details** table are:


Device Details	Description
Status	The status of fetching device rules/access control of the Firewall device
Devices Name	The names of the devices for which the rules will be fetched
Virtual FWs	For multi (vdom/context) Firewall, this will display the number of vdoms/contexts associated to this specific device rule. Clicking on the


Device Details	Description
	count will show the details of the vdoms/contexts individually. Refer the screen shot below.
Edit	An icon to edit the details of the rules fetching info of the device. Click icon to edit the device info.
View Rules	An icon to view the rules fetched from the device. Click icon to view the device rules.
Unused Rules	An icon to view the rules fetched from the device, which were not used. Click icon to view the unused rules of the device.
Compliance Reports	The Compliance Reports related to Firewall Rules/Policies Configuration/Changes The report is available on clicking the link and the link text shows the time the compliance report was generated. You can instantly generate the Compliance report by clicking the icon.
Last Update On	The time when the rules of the device were updated last.

Virtual FWs

- When you click the Virtual FWs number displayed in the **Device Details** list you will see the details of the virtual domains in a pop-up window which will provide you with all the options (see screen shot below).

admin Firewall's Virtual Domains				
VDOM Name	Rules	Compliance Reports	View Config Changes	Delete Rule/Config Fetching
CustA	 	2011-12-17 18:15 	- 	
CustB	 	2011-12-17 18:15 	- 	
admin	 	2011-12-17 18:16 	- 	

 **Quick Note**



- This page displays the list of virtual firewalls(for which device rule is configured) for corresponding device. If you don't want to fetch the rules/configuration for any specific vdom/context, you can do it by clicking the delete icon 
- For on demand fetching/viewing the rules or configuration or compliance report for a specific vdom, click on the corresponding icons shown next to the vdom name.




List Profile

Device Profile Listing

Click the **List Profile** link to view the list device profiles to fetch the rules information from the devices. The **Device Profile Listing** screen opens up.

On the top, there are links provided to add device info to fetch rules and to delete the device info. The links are:

-  Device Info
-  Profile

- c.  Assign Profile
- d.  Delete Profile
- e.  List Device Info

After creating and saving the Device Profile values through the Firewall Analyzer GUI, the profiles, edit option, view/associate profile with devices to fetch rules, is listed in the **Device Profile Details** table. The details of the columns of the **Device Profile Details** table are:

Device Profile Details	Description
Profile Name	The names of the profile, which will be used by the Firewall Analyzer to fetch the rules from the devices.
Edit	An icon to edit the profile details. Click icon to edit the device profile info.
View/Associate Devices	An icon to view the devices associated with the profile. Click icon to view the associated devices. If no device is associated, you will be prompted to associate a device.

Delete Profile

- To delete the Device Profile from the list of Device Profile Details table, select the check boxes of the respective Device Profile entries and click the **Delete Profile** link.

Add Device Info Profile


Click the **Add Device Info Profile** link or **New Profile** link to create device info profiles to fetch the rules information from a set of common devices. The **Add New Profile** screen pops up.

You can configure the individual device credentials to fetch the rules from the device or you can create a common profile of device credential which can be used for a group of devices to fetch rules.

- Enter the name of the new profile in the **Profile Name** field. Enter the description of the profile in the **Profile Description** text area.
- Select the protocol (Telnet or SSH) in the **Protocol** drop down list.
- Enter the Device Profile Info. The Device Profile Info has been split into two sections:
 - Primary Info** - deal with parameters that are necessary to establish communication with a common set of devices. Details such as Login Name, Password, Prompt, Enable UserName, Enable Password and Enable Prompt are classified as basic details.
 - Secondary Info** - certain parameters usually take standard values. All such parameters have been classified under 'Secondary Info'. Port, login prompt, enable user prompt, password prompt, enable password prompt values are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

Primary Info

Device Info	Description
Login Name	While establishing connection with a common set of devices, if the devices ask for a Login Name, set a value for this parameter. This parameter is Optional.
Password	To set the Password for accessing the common set of devices.
Prompt	The prompt that appears after successful login.
Enable UserName	When entering into privileged mode, some common set of devices require UserName to be entered. Provide the username if prompted; otherwise leave this field empty.
Enable Password	This is for entering into privileged mode to perform configuration operations like backup/upload. This parameter is mandatory.
Enable Prompt	This is the prompt that will appear after going into enable mode.

	Both Primary and Secondary credentials (Login Name and Password) of the Firewalls are encrypted and stored in the Firewall Analyzer.
---	--

Secondary Info

Click the link **Secondary Info** to view/enter values for these parameters. All the parameters are usually assigned with certain Standard Values by default. Such standard values have been filled for these parameters. Most of the devices would work well with these values and you need not edit these details unless you want to provide different set of details.

Device Info	Description
Port (Telnet/SSH)	Port number of Telnet/SSH - 23 (for Telnet) and 22 (for SSH) by default.
Login Prompt	The text/symbol that appears on the console to get the typed login name is referred as login prompt. For example, Login:
Password Prompt	The text displayed on the console when asking for password. For example, Password:
Enable User Prompt	The text displayed on the console when asking for Enable UserName. For example, UserName:
Enable Password Prompt	The text displayed on the console when asking for password. For example, Password:
Select Device Type	Select the type of device (Cisco/Fortigate/Netscreen) from the drop down list.

- The command to be executed, to fetch the Firewall rules is displayed in the **Command** field.
- Click **Save** button to apply the values to the device info profile. Click **Cancel** to cancel the adding device profile info operation.

Assign Profile


Click the **Assign Profile** link to associate devices to device profiles to fetch the rules information from the devices. The **Associate Profiles to Devices** screen opens up.


1. In the **Selected Profile** combo box, select the profile to be associated with the devices. If there is no profile available or you want to create and use a new profile, click **New Profile** link besides the combo box.
2. If you want to fetch the rules/configurations from the individual virtual Firewalls (virtual domain) separately, select the option '**Display Virtual Domains in the below resources list.**' It lists both the virtual Firewalls (virtual domain) and the physical devices in the **Unassigned Devices & Assigned Devices** list.
3. Select the devices, which you want to assign/re-assign to the selected profile. All the available devices are listed in the **Unassigned Device(s)** list. Select the devices and click right arrow. The selected devices are moved to the **Assigned Device(s)** list. If you want to remove any device from the **Assigned Device(s)** list, select the devices and click left arrow. The removed devices will be moved back to the **Unassigned Device(s)** list.
4. **Fetch Rules**
 - o Select whether the rules are fetched once or periodically.
 - o Select **Once** radio button to fetch the rules once.
 - o Select **Periodic** radio button to fetch the rules periodically. The periodicity option opens up. Select the periodicity of rules fetching from the combo boxes given in: **Every <1 to 31> day(s) @ <0 to 23> Hrs <0 to 50> Min.** (For example: If you configure like **Every 10 day(s) @ 2 Hrs 30 Min**, the rules will be fetched from the device, every 10 days at 02:30 AM)
5. **Compliance Reports**

The Compliance Reports related to Firewall Rules/Policies Configuration/Changes.

6. Click **Map** button to assign the selected devices to the selected profile. Click **Cancel** to cancel the assigning devices to the profile operation.

After associating the devices to Device Profiles the profiles and the associated devices are listed in the **Device Profile Details** table.

	<p>Getting Rules/ Configuration Information from the individual virtual Firewalls (virtual domain)</p> <p>If you want to fetch the rules/configurations from the individual virtual Firewalls (virtual domain) separately, select the option '<i>Display Virtual Domains in the below resources list.</i>' in Associate Profiles to Devices page. It lists both the virtual Firewalls (virtual domain) and the physical devices in the Select Device drop down list.</p>
---	---

	<p>Trouble Shooting: If the following message appears in the Compliance Reports field, enable Nipper.</p> <p><i>'Unable to generate compliance report. Reason: failed to locate nipper. Click here to enable it'</i></p>
---	---

Procedure to enable Nipper

In the Compliance Report field, the following message appears: *'Unable to generate compliance report. Reason: Failed to locate Nipper. Click here to enable it'*. What should I do?

Supported Platform:

- Ubuntu 9.1.10
- Fedora 12
- OpenSuSE 11.2
- CentOS 5.5

Prerequisite:

The GNU/Linux platform requires Qt 4.5 to be installed. Your package manager system should automatically install this for you.

Steps:

1. Download Nipper libraries from <http://www.manageengine.com/products/firewall/download-third-party-utilities.html> according to your platform
2. Install the rpm or deb according to your Operating System
3. Connect to Firewall Analyzer web client and type the following URL: '<http://<host name>:8500/fw/userConfig.do>'
4. In that, there is an option to provide the path in which you have installed 'Nipper'. For ex: `'/usr/bin/nipper'`
5. Click on **Save** link

After performing the above steps, go to **Setting > Device Rule > Add Device Info**, the option to generate compliance report for the device will be enabled.

Diagnose Firewall Connections


Firewall Analyzer allows you to diagnose the active connections passing through the firewall device. You can do it by clicking **Diagnose Connections** link that is provided in the **Settings** page.



This feature is available only for Netscreen and Cisco devices.



Firewall Analyzer uses Telnet/SSH protocol to login to the Firewall device and fetches the active connections passing through the Firewall.

Carry out the procedure given below to diagnose the Firewall connections:

1. In the Firewall Analyzer web client, select the **Settings** tab.
2. In **Settings** screen, select the **System Settings > Diagnose Connections** link. **Diagnose Firewall Connection** page appears.
3. In that page, select the Device Name, Device Type, Login Profile and Define Criteria.
 - a. Select the **Device Name** from the drop down list. Only the Netscreen and Cisco devices will be listed.
 - b. Select the **Device Type** (PIX, ASA, FWSM) from the drop down list, in the case Cisco devices. This field is not available for other devices.
 - c. Select the **Login Profile** from the drop down list. Choose an existing profile or add a new profile by clicking  icon beside the drop down box. Carry out the procedure given in the Add New Profile document.



- If a credential profile is already associated for the device, Firewall Analyzer will not prompt you to enter the device **Login Profile**.
- If a credential profile is not associated for the device, you can choose a credential profile to login to the Firewall device using Telnet/SSH. However, the profile chosen will be retained and used only for 'Diagnose Connection' purpose. To associate the login profile to this resource so that the settings will be retained in all other features, go to **Settings** screen, select the **System Settings > Device Rule > Assign Profile** link. You have to use the procedure given in the Assign Profile document.

- d. Define the criteria to fetch the connection for diagnosis using **Define Criteria** drop down list. The criteria are **IP Address**, **Between IPs**, **Protocol**, and **Port**. Enter the value in the text box besides 'is' text. By default only one criteria is displayed. To add more criteria, click  **Add** link and to remove criteria click  **Remove** link.



Specify the filter criteria to fetch the active connections from the Firewall device.


To reduce the load on Firewalls, Firewall Analyzer does not fetch all connections. It fetches upto 1000 random connections. If the connections goes beyond 1000 in number it will indicate at the bottom of the connections table.

You can add more criteria or redefine the criteria to reduce the results.


4. Click **Fetch Connections** to fetch the connections for diagnosis. The result will be displayed at the bottom part of the screen.





Scheduling Reports

Once you have created a custom report profile, you can set up schedules to run the report automatically at specified time intervals. You can also configure Firewall Analyzer to automatically email the report once it runs.


 Scheduled reports are generated and emailed only as PDF files. If you are viewing PDF reports on a Windows machine, make sure you have Adobe Acrobat Reader installed.

Click the **Schedule Listing** link under the **Settings** tab takes you the All Schedules page to view the list of reports that have been scheduled so far. The list shows all the schedules that have been set up so far, along with the report profile they are associated with, the type of schedule, and options to delete the schedule.

Click the  icon to delete a schedule. The report profile associated with this schedule will no longer be generated automatically at the specified time interval.


The  icon against a schedule is a toggle icon used to enable or disable a schedule. When the  icon is displayed, the schedule is enabled, and reports will be generated automatically for that schedule. Click the  icon to disable the schedule. The  icon is displayed indicating that the schedule is currently disabled. Reports will not be generated automatically for this schedule.

Creating a New Schedule

Click the  icon or the **New Schedule** link to add a new schedule. In the Add New Schedule page that comes up, enter the following details:

Attribute	Description
Task Name	Enter a unique name to identify this schedule
Profile Name	Choose the report profile to which this schedule has to be applied. All the report profiles that have been created are listed.
Mail Id	The first time a schedule is associated with a report profile, you need to enter the e-mail address to which the report has to be sent. Enter multiple e-mail addresses separated by a comma(,).
Hourly*	If you want to schedule this report to run every hour, enter the date and time after which this report has to run every one hour
Daily*	If you want to schedule this report to run every day, enter the date and time after which this report has to run every one day
Weekly*	If you want to schedule this report to run every week, enter the date and time after which this report has to run every one week
Monthly*	If you want to schedule this report to run every month, enter the date and time after which this report has to run every one month
Once only*	If you want to run this report only once, enter the date and time when the report has to be generated

* Choose from any one of these options

For **Daily**, and **Only once** schedules, you can set the  **TimeFilter** for **Custom Hours**, **Only Working Hours**, or **Only NonWorking Hours**.

For the **Daily** schedules, if the option **Run on Week Days** is selected then the reports are run daily except on the weekends. For the **Weekly** or **Monthly** schedules, select the option **Generate Report only for Week Days** if you want to report on the events that occurred only on the week days and not report on events that occurred over the weekends.

Once you have chosen all the required values click **Save Task** to save and activate the new schedule. Click **Cancel** to return to the All Schedules page.

Working Hour Configuration

Here you can configure the Working and Non-Working hour patterns of your enterprise. This will help you to distinguish between the working and non-working hour firewall log trends. By default, 10 - 20 Hours are considered as Working Hours and the remaining hours are considered as Non working Hours.

Two options are provided for configuring the working hour patterns.

- **General**

Here you can mention the **Start Time** and **End Time** for your official working hours, and all hours outside the given range is considered as non-working hours.

- **Advanced**

This option provides more customized working hours classification. For example, you may mention intermittent working hours like 8-12, 15-18, 19, 20, 21 Hours. Which means your non-working hour are 12-15 Hours and 21-8 Hours.



Working hour and Non-Working hour traffic details for external hosts (hosts outside the LAN) will not be available in the Firewall Analyzer reports.

Report View Customization

Here you can customize the device specific reports to be shown in Device Tree and the Reports page.

For each of the selected device, you are provided with the option of selecting from the default **Available Reports** the most required list of reports and move it to the **Selected Reports**. And only these selected reports would be listed in the Device Tree and the Reports page for this device.

You can customize images used in the PDF Reports.

Select the **Customize images for PDF Reports** check box. The **Cover Image** and **Footer Image** text boxes and **Browse** buttons will become active. There will be an icon besides the **Cover Image** and **Footer Image** texts. Clicking on the icons will display the thumb nail (with dimensions) of the default/current image. Below the text box, dimension of the default/current image will be displayed. Select the new images using the **Browse** buttons.

Customize images for PDF Reports	
Cover Image:	Size: 612px(width) X 820px(Height)
Footer image:	Size: 547px(width) X 37px(Height)

The report view customization for the selected device can be applied on the selected device alone by clicking **Apply for Selected Device**. And, if you would like the report view customization for the selected device to applied for all other devices too then click **Apply for All Device**.

Rebranding Firewall Analyzer Web Client

To customize the Firewall Analyzer Web Client follow the steps given below:

1. In the Firewall Analyzer web client, select the **Settings** tab.
2. In **Settings** screen, select the **System Settings > Rebranding FWA Web Client** link. Rebranding **Firewall Analyzer Web Client** page appears.

The **Rebranding FWA Web Client** link lets you to customize all the logos, images, and links used in the Firewall Analyzer Web Client to suit the needs of the MSSPs (Managed Security Service Providers).

The rebranding screen contains two sections. At the top you have the **Customize Images** section. In this section, you can customize logos and images. At the bottom you have the **Customize Strings/Links** section. In this section, you can customize strings and links.

Customize Images

Replace the default images with your company/enterprise images


Client Logos & Images	Where it is used	Image Size & Thumbnail	New Image
Company Logo	Login Page	129*39 pixels	
Product Logo	Login Page	289*59 pixels	
Top Band Image	Client Header	232*47 pixels	
PDF Cover Image	PDF Cover Page	612*820 pixels	
PDF Footer Image	PDF Footer	547*37 pixels	
Server Status Image	Tray Icon [Windows]	400*60 pixels	

Customize Strings/Links

Replace the default strings/links with your company/enterprise strings/links

Client Strings & Links	Where it is used	Existing String/Link	New String/Link
Company Name	Login Page	Zoho Corp.	
Brand Name	Login Page	ManageEngine	
Company Website	Login Page	www.manageengine.com	
Product Website	Login Page	www.fwanalyzer.com	
Support E-Mail	Login Page	fwanalyzer-support@manageengine.com	
Sales E-Mail	About Popup	sales@manageengine.com	

Click **Update** to update the customized images/logos and strings/texts. Click **Cancel** to cancel the customizing the web client operation.

	<ul style="list-style-type: none">• You can customize ZohoCorp/ManageEngine images/links as per your requirement.• Customization takes effect only for the changed images/links, else default images/links are retained.• Size of new image should be of same size as the default image.• Images with the following file extensions are only permitted: .jpg, .gif, and .png
---	--

Admin Settings

Managing Protocol Groups

A protocol group is a set of related protocols typically used for a common purpose. The **Protocol Groups** link lets you define protocols as well as protocol groups, so that you can identify traffic that is unique to your enterprise. Most of the common enterprise protocols are already included in Firewall Analyzer under appropriate groups.


Some of the important protocol groups include the following:

Protocol Group	Protocols Included	Description
Web	HTTP, HTTPS, Gopher	Includes protocols used to access IP traffic (the Internet)
Mail	POP, SMTP, IMAP	Includes protocols used to send or receive e-mail traffic
FTP	FTP, TFTP, FTPS	Includes protocols used to transfer files through FTP
Telnet	telnet	Includes protocols used to access telnet services



Click the **Protocol Groups** link to view the list of protocol groups and the corresponding protocols.



The **View by Group** box lets you view the list, one protocol group at a time.



The **Unassigned** protocol group contains all the protocols that are not assigned to any group.

	Some firewalls interpret protocols at Layer 4 (Application Layer), which means that a combination of port and protocol is identified as an application, and written into the log file. For example, <i>tcp</i> protocol on port <i>80</i> is identified as <i>http</i> traffic. Hence <i>http</i> is shown in the Protocols column. Other firewalls interpret protocols at Layer 3 only, which means only the port and protocol values are written into the log file. Hence, in the same example, <i>tcp/80</i> is shown in the Protocols column.
---	---


Operations on Protocols

Click the  icon next to a protocol to delete it from the protocol group. Once a protocol is deleted, all the database records related to that protocol will be deleted. Click the  icon to move a protocol from the current protocol group to another.


Click the **Add Protocol** link or the  icon next to it to add a new protocol, and assign it to a protocol group. Remember to enter the protocol value exactly as it appears in the log file. If you want to add it to a new protocol group, click the  icon next to the Protocol Group text box to add a New Protocol Group, and enter the name of the new protocol group and click **Add**. From the list of **Available Protocol Identifiers**, move the required protocols to the **Selected Protocol Identifiers** to be included in this protocol group. Please note that a protocol can belong to only one protocol group at a time.


Click the **Add Protocol Identifier** link or the  icon to add a new protocol identifier. And, to specify the range for the protocol identifier click the **Add Protocol Identifier Range** link or the  icon and specify the From Port & To Port of the protocol identifier, and select between tcp or udp for the Layer 3 Protocol.




When you see the  icon next to the *Unassigned* protocol group on the Dashboard, you need to add the protocols and assign them to protocol groups in this way.



Operations on Protocol Groups


Click the **Add Protocol Group** link or  icon next to it to add a new protocol group. In the popup window that opens, enter a unique group name, and a short description. From the list of protocols currently not assigned to any protocol group, choose the protocols to be included in this protocol group. Please note that a protocol can belong to only one protocol group at a time.


Select the protocol group from the list and click the **Edit Protocol Group** or the  icon to edit the properties of that protocol group. In the popup window that opens, you can edit the protocol group's description, add currently ungrouped protocols, or remove existing protocols from this protocol group.

To delete a protocol group, select the protocol group from the list and click the **Delete Protocol Group** link or the  icon next to it. The protocol group is deleted, and all associated protocols are put in the **Others** protocol group.

Operations on Protocols


Click the **Add Protocol** link or  icon next to it to add a new protocol. In the popup window that opens, enter a unique protocol name. From the list of protocol groups currently available, choose the protocol group to which this protocol needs to be included. You can also add new Protocol Group to assign this Protocol, using  icon next to Protocol Group combo box. Please note that a protocol can belong to only one protocol group at a time. From the list of **Available Protocol Identifiers** currently available, choose the Protocol Identifiers to be included in this Protocol, send it to the **Selected Protocol Identifiers** list. You can add new Protocol Identifiers, as per your requirement, using **Add Protocol Identifier** link. You can add new range of ports for the selected Layer 3 Protocol as Protocol Identifiers, using **Add Protocol Identifier Range** link. Click **OK** button to complete the operation and **Cancel** button to abort the operation.

Select the protocol from the list and click the **Edit Protocol** or the  icon to edit the identifiers of that protocol. In the popup window that opens, you can edit the protocol's identifiers, add new protocol identifiers, or remove existing protocol identifiers from this protocol.

To delete a protocol, select the protocol from the list and click the **Delete Protocol** link or the  icon next to it. The protocol is deleted, and all associated protocol identifiers are put in the **Available Protocol Identifiers** list.

How to group the unassigned Protocols

Generally used protocols like Mail, Web, FTP, Telnet, etc., have been configured as Groups. However, the unknown protocols can be grouped as per your requirement.

1. Click on the '**Unassigned**' in protocol group under Traffic Statistics, which shows all the unknown protocols.
2. Click on Assign and Select 'All' under Hits and select the 'Multiple Selection', which lists all the unassigned protocols.
3. Select the protocols and group it under protocol group and assign the appropriate protocol.
4. If you do not find a protocol group, click on the  sign to add a new protocol group.

Once you configure the protocols to protocol groups, you will not receive any unassigned protocol after the time of assigning. Once you assign the protocols, the reports will show the assigned protocols only from the assigning time. Hence, in the reports generate earlier to the protocol assignment, you will see only the unassigned protocols and in the upcoming reports, you can find the newly assigned protocols under their appropriate protocol group.

If you are not sure of the protocols, which needs to be assigned, kindly check the application that uses the port/protocol. You can also check the raw log in the *<Firewall Analyzer Home>\server\default\archive\<firewall IP address>* folder.

Setting up Intranets

Firewall Analyzer includes the option to specify networks, or a range of IP addresses to identify machines behind a firewall. This setup is identified as the Intranet. By adding the machines or IP addresses that are located within your network (LAN), you can identify and distinguish between traffic that is generated within your network, and traffic that is coming from, or destined outside your network.

Click the **Intranet Settings** link to define intranets. The Intranet Settings page will list all the devices that have been configured to send their logs to Firewall Analyzer for analysis.

The **Change** action, found against each listed firewall, would enable you to configure the (intranet) private **IP Network / IP Address / IP Range** for each firewall.

For instance, if you are a MSSP (Managed Security Service Provider) who is monitoring firewalls of different client networks at different locations and all your clients could possibly end up with the same (intranet) private **IP Network / IP Address / IP Range**, then **Configure all devices** would serve the purpose of applying the common configuration across **All Devices**.

- To designate an entire IP network as an Intranet, select **IP Network** from the list, and enter the network IP address and the corresponding Net Mask value.
- To include a single host in the Intranet, select **IP Address** from the list, and enter the IP address of the host.
- To designate a range of IP address as the Intranet, select **IP Range** from the list, and enter the starting IP address and the ending IP address.



For Example : If you have three private **IP Network** (say) 10.8.0.0, 10.9.0.0, and 10.10.0.0, each with Net Mask: 255.255.0.0, then instead of adding them separately, we would recommend you to give the entire private IP network : 10.0.0.0 with Net Mask 255.0.0.0, as this would improve the performance of Firewall Analyzer. The same is recommended for **IP Range** too, where you can mention Start IP: 10.0.0.0, End IP: 10.255.255.255. And this is applicable to Class B & Class C networks too!

You can specify multiple intranets by clicking the **Add** button. Once you are done, click **Save Settings** to activate the new settings.

Adding Different Users

Click the **User Management** link to create and manage the different users who are allowed to access the Firewall Analyzer server.

The different types of users and their respective privileges are described in the table below:

User	Description
Administrator	This user can do all operations including configuring syslog servers, setting up file archiving, adding additional users, and more
Operator	This user can do all operations except configuring the Intranet settings, and user management
Guest	This user can only view reports, view device details, and basically has only read-only privileges. The Alerts, Ask Me & Support tabs are not available for guest users.

By default, an Administrator user with username as **admin** and password as **admin**, and a Guest user with username **guest** and password **guest** are already created.

If you have logged in as an Administrator user, the **User Management** page lists all the users created so far.

You can view the users based on user type. Select the user type from the **Select User Type** combo box. The three user types listed are: *Administrator*, *Operator*, and *Guest*.

You can view the users alphabet wise. **All** option and the alphabets are listed above the user list. Select **All** option or the alphabet under which the user login name will be available.

Viewing Login Details

If you have logged in as an Administrator user, click the User Audit **View** link against a user to view the corresponding user audits. The **User Audit** page shows the remote host IP address from which the user logged on, the timestamp of the login, and the duration of the session.

The description the user details available in the user list table are explained below:

User Detail	Description
User Name	The user's login name
No. of HostGroups	The number of host group(s) to which the user will be having access
Access Level	The access level privilege of the user
Domain Name	The domain in the network to which the user belongs to
User Audit	The corresponding user audits information

Delete

Select all users check box if you want to delete all the users and individual user(s) check boxes to delete the selected users. There is a check box against each user below the all user check box. Click **Delete** button to delete all the or selected user(s) from the list of users accessing Firewall Analyzer.

Assign Role

Select the users for whom the host group(s) need to be assigned/re-assigned. Select the access level of the user from the **Access Level** combo box. The three access levels listed are: *Guest*, *Operator*, and *Administrator*. Click **OK** to save the new changes. Click **Cancel** to cancel assigning the role operation.

Assign Group(s)

Select the users for whom the host group(s) need to be assigned/re-assigned. Select the host group to which the user will be having access. All the available host groups are listed in the **Available HostGroup(s)** list. Select the host groups and click right arrow. The selected host groups are displayed in the **Selected HostGroup(s)** list. If you want to remove any host group from the **Selected HostGroup(s)** list, select the host groups and click left arrow. The removed host groups will be listed back in the **Available HostGroup(s)** list.

Adding a New User

- Click the **Add New User** link to add another user to access Firewall Analyzer.
- Enter the new user's login name in the **User Name** text box. The user name should be unique. If you want the user name as password, select the **Use Login Name as Password** check box.
- Enter the user's password in the **Password** text box. The password should be of 5 to 20 characters long.
- Re-enter the user's password in the **Verify Password** text box.
- Select the access level of the user from the **Access Level** combo box. The three access levels listed are: *Guest*, *Operator*, and *Administrator*.
- Enter default e-mail address the user in the **Email Address** text box.
- Select the host group to which the user will be having access. All the available host groups are listed in the **Available HostGroup(s)** list. Select the host groups and click right arrow. The selected host groups are displayed in the **Selected HostGroup(s)** list. If you want to remove any host group from the **Selected HostGroup(s)** list, select the host groups and click left arrow. The removed host groups will be listed back in the **Available HostGroup(s)** list.
- Click **Add User** to add this user to the list of users accessing Firewall Analyzer. Click **Cancel** to cancel the adding user operation.

Editing User Details

If you have logged in as an Administrator user, the **User Management** page lists all the users created so far.

- Click the **Edit** link to edit the user details. You can change the access level, password, and optionally, the default e-mail address for this user.
- You can edit the host groups associated with the user. Select the host group to which the user will be having access. All the available host groups are listed in the **Available HostGroup(s)** list. Select the host groups and click right arrow. The selected host groups are displayed in the **Selected HostGroup(s)** list. If you want to remove any host group from the **Selected HostGroup(s)** list, select the host groups and click left arrow. The removed host groups will be listed back in the **Available HostGroup(s)** list.
- Once you are done, click **OK** to save the new changes. Click **Cancel** to cancel editing the user operation.

OR

If you have logged in as an Operator or Guest user, click on the **Account Settings** link to change your password and default e-mail address.

Once you are done, click **OK** to save the new changes. Click **Cancel** to cancel editing the user operation.

Firewall Analyzer User Privileges

Types of User Privileges in Firewall Analyzer

- **Administrator** - Can perform Add/Edit/Delete operations of all product configurations and Firewalls.
- **Operator** - Can perform Add/Edit/Delete operations of the Firewalls assigned to him and product configurations except Intranet Settings and User Management.
- **Guest** - Has read-only privileges for the Firewalls assigned to him and cannot perform any product configuration.

Comparison of Feature Access to the Users

Sl No	Feature Name	Administrator	Operator	Guest
1	User Management Create/Modify/Delete users	Yes	No	No
2	Predefined Reports and ReportProfiles	The user can view all predefined reports of all the firewalls. The user can perform Add/Edit/Delete operation of Report profiles created by	The user can view all predefined reports of Firewalls assigned to him. The user can perform Add/Edit/Delete operation of Report profiles created by	The user can view all predefined reports of Firewalls assigned to him. The user can view all report profiles of Firewalls

SI No	Feature Name	Administrator	Operator	Guest
		all users.	himself.	assigned to him.
3	Alert Profiles and Alert Administration	The user can perform Add/Edit/Delete operation of Alert profiles created by all users. Administration of Alerts created by All Alert Profiles	The user can perform Add/Edit/Delete operation of Alert profiles created by himself. Administration of Alerts created by his own Alert Profiles	The user can view all the generated alerts of Firewalls assigned to him.
4	Edit/Delete Device	All Firewalls	Only for Firewalls assigned to him.	No
5	Dashboard View Customization	For all Firewalls	Only for Firewalls assigned to him.	Only for Firewalls assigned to him
6	Advanced Search	Yes	Yes	The user can perform advanced search except Save as Report Profile.
7	Intranet Settings Configuring Firewall based LAN settings	Yes	No	No
8	Bookmark	The user can view only his bookmarks.	The user can view only his bookmarks.	The user can view only his bookmarks.
9	Configuration Settings listed in the Settings tab. <ul style="list-style-type: none"> Adding Syslog Server Check Point Firewall Settings Alert Profiles view Import Log files view Schedule Listing page Working Hour configuration Customize Report Tree Mail Server 	Yes	Yes	No

SI No	Feature Name	Administrator	Operator	Guest
	Settings <ul style="list-style-type: none"> Database Console 			
10	Configuration views present in the Settings Tab. <ul style="list-style-type: none"> Device Details Archived Files Protocol Groups Server Diagnostics Account Settings 	Yes	Yes	The user can view all the Configuration settings except Archive Settings and Server Diagnostics .
11	User Assistance <ul style="list-style-type: none"> Tell a Friend Upgrade License Help Feedback About 	Yes	Yes	No


Setting up the Mail Server

You need to configure the mail server on Firewall Analyzer in order to receive email alert notifications and scheduled reports.

Click the **Mail Server Settings** link to edit the mail server settings. Enter the following details:

Field	Description
Outgoing Server Name	Enter the name of the SMTP server on your network which is used for outgoing emails.
Port	Enter the port used by the SMTP server. Usually this is 25.
Authenticate for every Login	If your SMTP server requires you to authenticate yourself before sending an email, check this option. Otherwise leave it unchecked. * The below two fields are active only when this checkbox is checked.
User Name*	Enter the user name used to authenticate email sending from this machine.
Password*	Enter the corresponding password for the typed user name.
Use Secure Connection	Select the TLS button to secure the connection between mail server and FWA server. Select No button if secure connection is not required.
Sender MailId	Enter the Sender or From Address which needs to be mentioned in the outgoing emails. By default, <i>firewallreport@localdomain.com</i> will be mentioned as the sender mailid. The Test Server button is for testing the mail server configurations. You can give your email-id in the "Enter Recipient Mail Id" field, which comes-up when you click Test Server. If the mail server configurations have been given correctly you will receive a Test Mail.

After all the details have been filled in, click **Save Changes** to save the mail server settings.

	<ul style="list-style-type: none"> If you want to send secured emails, you can use the Use Secure Connection option. The Transport Layer Security (TLS) option uses public key encryption to send the email to untrusted networks. For more information on Transport Layer Security (TLS) refer the URL: http://en.wikipedia.org/wiki/Transport_Layer_Security. Also refer the link to know about TLS http://technet.microsoft.com/en-us/library/cc784450%28WS.10%29.aspx If the mail server is not configured, you will see an error message when you are setting up an email alert notification or scheduling a report to be emailed automatically. Click the Configure Mail Server now link inside the error message to configure the above settings from the opened popup window.
---	--

External Authentication Settings

Firewall Analyzer provides two more external authentication apart from the local authentication. They are **Active Directory** authentication and **Remote Authentication Dial-in User Service (RADIUS)** authentication. If you import users from Active Directory or if you add a RADIUS server details, you will find the **Options >>** link besides the **Login** button in the Firewall Analyzer Client UI Login screen. If you click the **Options >>** link, **Log on to** field will appear below the **Password** field. The Log on to field will list the following options:

- **Local Authentication** - If the user details are available in local Firewall Analyzer server user database
- **Radius Authentication** - If the user details are available in RADIUS server and dummy user entry should be available in local Firewall Analyzer server user database
- **Domain Name(s)** - If the details of the user of a domain is imported from Active Directory into the local Firewall Analyzer server user database

Enter the **User Name** and **Password**. Select one of the three options in **Log on to** (**Local Authentication** or **Radius Authentication** or **Domain Name**). Click **Login** button to log in to Firewall Analyzer Client UI.

Active Directory Configuration Settings

Users in the AD (Active Directory) can be imported into Firewall Analyzer server. You have to select the required OUs (Organizational Units) under the Listed domains. You can re scan the network to find domains. Login to individual servers of the domain to get the OUs listed and select the OUs as per your requirement. Use the server credentials (User Name & Password) to login to the server. For the first time, all the users will be imported into Firewall Analyzer. On subsequent or periodic imports, only the new user added to the AD will be imported.



The imported users will be added in the Firewall Analyzer server with the following constraints:

Access Level as *Operator* and will have access to all the Firewall devices.

Procedure to configure AD settings

Click the **External Authentication Settings** link under the **Settings** tab to configure the AD user details import, periodic import, and to enable user authentication usage. On clicking the **Active Directory** tab, the **Active Directory Configurations** page opens up. In that page, you will find the following sections:

- Import users from Active Directory
- Schedule
- Authentication

Import users from Active Directory

In this section, you will find **Import Users** button. Click the button and **Import users from Active Directory** screen pops-up.

In that screen, you will find the following items:

- **Domain Name** combo box & **Rescan Network** link

Domain Name combo box will list all the available domains in the network. Besides the combo box, you will find the **Rescan Network** link. Clicking the link will re scan the network to find out all the available domains. Select the domain from the combo box as per requirement.

- **Server Name**

If you want to list the OUs of a particular server, enter the server name in the text box.

- **User Name**
- **Password**

If you want to access a server and get list of (Organizational Units) OUs, enter the user name and password of the server in the text boxes.

- **Login & List OUs** button

After entering the server name to be accessed and the credentials for server access, click this button to get the list of (Organizational Units) OUs.

- **Cancel** button

If you want to cancel the access to server and get list of OUs operation canceled, click this button.

Schedule

In this section, you will find a check box to schedule the import of users periodically from AD and a Save button.

every __ days" check box. Enter the periodicity of user import in days.

Click **Save** button to save the changes.

Authentication


In this section, you will find the status (**Status: Disabled**) of the AD authentication to be used for users imported from AD and Enable button.

Click **Enable** button to use AD authentication for the users imported from AD. On clicking the button the status will change to **Enabled (Status: Enabled)** and the **Enable** button will change to **Disable**.

RADIUS Server Configuration Settings

You can also leverage the RADIUS authentication for user access bypassing the local authentication provided by Firewall Analyzer.

In the RADIUS server authentication the users credentials are sent to the RADIUS server. The server checks for the user credentials and sends the authentication successful message to Firewall Analyzer server.

	Note: If the user has only RADIUS server authentication, create the user in Firewall Analyzer with dummy password. On user logging in with RADIUS server authentication, the dummy password in the local server is ignored and the user credentials are sent to RADIUS server for authentication. Refer the procedure given in the Adding Users document to add a new user with dummy password.
---	--

You can make Firewall Analyzer work with RADIUS server in your environment. This section explains the configurations involved in integrating RADIUS server with Firewall Analyzer.

Procedure to configure RADIUS server settings

To configure RADIUS server in Firewall Analyzer, provide the following basic details about RADIUS server and credentials to establish connection:

Click the **External Authentication Settings** link under the **Settings** tab to configure the RADIUS server configuration. On clicking the **Radius Server** tab, the configuration fields are displayed. In that page, you will find the following fields:

RADIUS Server Settings	Description
Radius Server IP	The IP Address of the machine in which the RADIUS server is running. Enter the IP address of the host where RADIUS server is running
Radius Server Authentication Port	The port used by the RADIUS server for authenticating users. Enter the port used for RADIUS server authentication. By default, RADIUS has been assigned the UDP port 1812 for RADIUS Authentication.
Radius Server Protocol	The protocol used by the RADIUS server for authenticating users. Select the protocol that is used to authenticate users. Choose from four protocols: <ul style="list-style-type: none"> • PAP - Password Authentication Protocol • CHAP - Challenge-Handshake Authentication Protocol • MSCHAP - Microsoft Challenge-Handshake Authentication Protocol

RADIUS Server Settings	Description
	<ul style="list-style-type: none">• MSCHAP2 - Version 2 of Microsoft Challenge-Handshake Authentication Protocol
Radius Server Secret	The secret string used for connecting RADIUS client (Firewall Analyzer) with the server. Enter the RADIUS secret used by the server for authentication
Authentication Retries	The number of retries the RADIUS server to permit for authenticating users. Select the number of times you wish to retry authentication in the event of an authentication failure


Setting up the Mail Server

You need to configure the mail server on Firewall Analyzer in order to receive email alert notifications and scheduled reports.

Click the **Mail Server Settings** link to edit the mail server settings. Enter the following details:

Field	Description
Outgoing Server Name	Enter the name of the SMTP server on your network which is used for outgoing emails.
Port	Enter the port used by the SMTP server. Usually this is 25.
Authenticate for every Login	If your SMTP server requires you to authenticate yourself before sending an email, check this option. Otherwise leave it unchecked. * The below two fields are active only when this checkbox is checked.
User Name*	Enter the user name used to authenticate email sending from this machine.
Password*	Enter the corresponding password for the typed user name.
Use Secure Connection	Select the TLS button to secure the connection between mail server and FWA server. Select No button if secure connection is not required.
Sender MailId	Enter the Sender or From Address which needs to be mentioned in the outgoing emails. By default, <i>firewallreport@localdomain.com</i> will be mentioned as the sender mailid. The Test Server button is for testing the mail server configurations. You can give your email-id in the "Enter Recipient Mail Id" field, which comes-up when you click Test Server. If the mail server configurations have been given correctly you will receive a Test Mail.

After all the details have been filled in, click **Save Changes** to save the mail server settings.

	<ul style="list-style-type: none"> If you want to send secured emails, you can use the Use Secure Connection option. The Transport Layer Security (TLS) option uses public key encryption to send the email to untrusted networks. For more information on Transport Layer Security (TLS) refer the URL: http://en.wikipedia.org/wiki/Transport_Layer_Security. Also refer the link to know about TLS http://technet.microsoft.com/en-us/library/cc784450%28WS.10%29.aspx If the mail server is not configured, you will see an error message when you are setting up an email alert notification or scheduling a report to be emailed automatically. Click the Configure Mail Server now link inside the error message to configure the above settings from the opened popup window.
---	--

Configuring Firewall Availability Alerts


In Firewall Analyzer, alert can be triggered, if the Firewall stopped sending the logs. The alert triggering is configurable. Firewall non-availability alert configuration notifies the user through e-mail, when the Firewall Analyzer is not receiving logs from firewall(s).

Follow the procedure given below to configure the triggering of alert:


- Select the **Settings** tab in the Web Client. On the right side of the screen, you will see **Admin Settings** section below the **System Settings** section. In the **Admin Settings** section, there will be **Firewall Availability Alert** link.
- Click the **Firewall Availability Alert** link. The **Firewall Availability Alert** page opens. In the screen, there will be a link **+Add Alert** on the left side top to add an alert. Below the link, the configured alerts are listed in a table. The details of the table columns are:

Columns	Description
Device Names	The device names of the firewalls, for which this alert will be triggered, if the firewalls fail to send logs.
Alert Mail Address	Failure of the above mentioned firewalls to send logs will trigger an alert to send e-mail to the configured users e-mail IDs.
Time Interval (minutes)	The time duration within which a log should be received by the Firewall Analyzer. Failure to receive a log within this time duration will trigger this alert.
Action	This indicates whether the configured alert is enabled or disabled.

- To configure an alert, click the **+Add Alert** link. The **Create Availability Alert** page opens.
 - Select the firewall devices for which this alert needs to be triggered using the **Change Selection** link. A pop-up window **Select Devices from the list** opens to select the devices. In this the first option will be **All Devices**, and below the **All Devices** option the devices are listed. Select the **All Devices** option or devices as per requirement. The selected devices are displayed under the **Selected Devices**.
 - In the **"If the logs are not received from the above selected firewall(s) for at least (15 minutes/30 minutes/60 minutes/2 hours/6 hours/12 hours/1 day)"** part, select the time duration from the combo box. The time interval options available are: 15 minutes, 30 minutes, 60 minutes, 2 hours, 6 hours, 12 hours, and 1 day.
 - Configure the following in the **Send Alert as** section:
 - Select the **Mail** check box.
 - Enter the e-mail address in the **Mail To** text box, to which the alert has to be sent. Enter multiple e-mail addresses separated by a comma(,).
 - Optionally, you can modify the e-mail subject in the **Subject** text box as per your requirement.

	<p>If the Mail Server is not configured the following note appears and there is a link provided to configure the Mail Server. Configure the Mail Server in order to get the mail alerts.</p> <p>Note: Mail Server is not configured. Click here to configure the Mail Server.</p>
---	---

- Select the **SMS** check box.
- Enter the mobile phone number in the **SMS To** text box, to which the alert has to be sent. Enter multiple phone numbers separated by a comma(,).

	<p>If the SMS Settings is not configured the following note appears and there is a link provided to configure the SMS Settings. Configure the SMS Settings in order to get the SMS alerts.</p> <p>Note: Mail Server is not configured. Click here to configure the Mail Server.</p>
---	---

- Select the **Run Script (SNMP)** check box.
 - Select the script to be run in the **Location** field. Click the **Choose File** button to browse the location of the script file. Besides the button, the selected file name will be displayed. If no file is chosen, **No file chosen** is displayed.
- After choosing all the required values, click **Add Alert** to save and activate the new alert. Click **Cancel** to cancel the alert configuration.

Viewing Server Diagnostics

Click the **Server Diagnostics** link to see server-specific device information. This information will be useful while troubleshooting the server or reporting a problem.

The various information boxes on this page are described in the table below:

Box	Description
License Information	This box shows details about the license that is currently applied.
System Information	This box shows device information for the Firewall Analyzer server
Installation Information	This box shows details about the Firewall Analyzer installation on the server machine
JVM Memory Information	This box shows statistics on the amount of memory used by the JVM

Accessing the Database

Firewall Analyzer lets advanced users access the in-built database and run standard queries.

Click the **Database Console** link to open the Database Console page. In the prompt window displayed, enter the query to be executed.

Remember the following when executing a query:

- Table names and table columns are case-sensitive.
- For SELECT queries, set the row limit between 1 and 500. Default row limit is 10.



Keep in mind that you are accessing the database directly at your own risk. Any update or delete operations will result in loss of data.

License Management - Manage/Unmanage Devices

Firewall Analyzer offers a powerful and rich feature to manage and unmanage the devices. It offers a greater degree of flexibility to manage the number of devices that can be monitored by using Firewall Analyzer.

Click the **Settings > Admin Settings > License Management** link to manage/unmanage/delete devices. On clicking the link **License Management** page opens up. On the right side top corner of the screen, you will find **Apply License, Buy Online, Tell a Friend** buttons with links. On top of the page, the details of the license you have purchased will be displayed.

License Details	Value	Description
Max Number of Devices :	50	Total number of device licenses purchased
Managed Devices :	33	Number of devices getting managed
Remaining Number of Devices :	17	Remaining number of device licenses available for managing devices
License Type :	Premium	Type of license i.e., Professional, Premium, Trial

Below the License Details you will find the list of devices currently added to the Firewall Analyzer for monitoring and their status of getting managed or unmanaged. The tabular list contains individual and select all devices check boxes. On top and bottom of the list, there are three buttons available for operations. The operations are **Manage**, **Unmanage**, and **Delete**. All the devices added to the Firewall Analyzer server will be listed in this page. From the list of added devices, select one or multiple devices using the check boxes against the respective devices. To select all the devices, select the check box in the table/list header.

Manage

Only the managed devices logs will be parsed and archived. Number of managed devices cannot exceed number of licensed devices. Select required device(s) or select all devices to manage. Click the **Manage** button. The selected device will be managed.

Unmanage

The unmanaged device logs will be dropped and not archived during the unmanaged period. As an ad-hoc option, if you want to manage a particular critical device and number of licensed devices is exceeding, you can unmanage less critical device(s) and manage the critically required device. We would recommend you to buy more device licenses to get uninterrupted performance. Select required device(s) or select all devices to unmanage. Click the **Unmanage** button. The selected device will be unmanaged.

Delete

Delete the devices from the list of devices. When the device(s) are deleted, all related information of the device(s) will be removed from the database. Select required

device(s) or select all devices to delete. Click the **Delete** button. The selected device will be deleted.



You can select multiple devices and manage/unmanage/delete them.

If you want to monitor Firewall device in High Availability mode, ensure that Firewall Analyzer is bound to one source (that is a single IP Address/host name), then that source is considered as one device license.



Note: Each Virtual Firewall (vdom) monitored separately will be considered as one Firewall device for license purpose. If the Virtual Firewall is combinedly monitored with physical device as one Firewall device source and not as separate Virtual Firewall, then the physical device source will be considered as one Firewall device for license purpose. You can configure this option in the product.

SMS Settings

The SMS setting is similar to Mail Server setting. You need to configure the SMS settings in order to send SMS alert notifications to your cellular phone.



This option is visible only for users with **Admin** and **Operator** access level

Click the **SMS Settings** link under the **Settings** tab to configure the port in which the SMS equipment is connected and mobile phone number to test the functioning of port.

On clicking the link, SMS Settings screen open up on the right hand side. In that you will see **GSM Communication Port Name** text box and **Test Port** button.

- Enter the communication port name (For example: **COM1**) in the text box.
- Click the **Test Port** button.
- On clicking the button, a window pops-up to enter phone number to test port.
- Enter mobile phone number with '+' sign and country code (For example: +19259249500).
- Click **OK** button. If the port & SMS equipment is functioning properly, you will get a test message on the phone. Click **Cancel** button to abort the testing.

Once you have entered the required port number and tested it, click **Save Changes** to save the changes. Click **Cancel** to return to the default **Settings** tab.



The phone number entered in the pop-up screen is meant only for testing the SMS port. Phone numbers to which the Alerts are to be SMS notified need to be configured in individual Alert profiles.

Supported Modems for SMS Notifications

Following is a list of the modems supported in ManageEngine products for SMS Notifications.

S No	Modem Version	Baud Rate	Manufacturer
1	Itegnio 3000	115200	Wavecom
2	Itegnio WM1080A	115200	Wavecom
3	Wavecom M1306B		Wavecom
4	MultiTech MultiModem MTCBA-G-F1		
5	Wavecom Fastrack M1206B	115200	Wavecom

Mobiles Supported

S No	Mobile Model	Baud Rate	Manufacturer
1	Motorola E398	9600	Motorola
2	Nokia 6210		Nokia
3	Nokia 6310		Nokia
4	Nokia 6230i		Nokia
5	Nokia 8250		Nokia
6	Nokia 6610	115200	Nokia
7	Nokia 7210	115200	Nokia
8	Sony Ericsson T610	19200	Sony Ericsson
9	Sony Ericsson W800i	115200	Sony Ericsson
10	samsung sgh-c100	9600	Samsung
11	Sharp GX30	115200	Sharp
12	Sony Ericsson k700	115200	Sony Ericsson
13	Motorola RAZR V3	115200	Motorola
14	Nokia 7610	115200	Nokia
15	Nokia 3310/3315	19200	Nokia
16	Siemens M35	19200	Siemens
17	Siemens M50	19200	Siemens
18	Siemens C45	19200	Siemens

Can't find the modem or the mobile you have in this list?

No worries! check whether the device, you have, meets the following configuration.



- Modem/ Mobile must have GSM functionality with a provision to insert the SIM card.
- Should support 7bit (GSM default alphabet), 8bit and Unicode (UCS2) encoding.
- Firewall Analyzer uses AT commands to send SMS, so the device should respond to AT commands. [If required, test using HyperTerminal]

If all the above criteria match, Firewall Analyzer will support your modem/ mobile phone.

Changing Account Settings

Click the **Account Settings** link under the **Settings** tab to change the default password and e-mail address set for this account. You cannot change the account's user name or access level.

Once you have made the required changes, click **Save User Details** to save the changes. Click **Cancel** to return to the default **Settings** tab.



This option is visible only for users with **Guest** or **Operator** access level

Configuring Firewalls

Firewall Analyzer listens at the default ports for exported log files. The following is a list of firewalls and versions for which configuration instructions are included. Click the firewall name to see the corresponding configuration instructions.

Firewall Name	Version Numbers
Check Point	log import from most versions and LEA support for R54 and above
NetScreen	Most version
Cisco Systems	Cisco PIX Secure Firewall v6.x, v7.x Cisco ASA Cisco IOS Cisco VPN 3000/3005 Concentrator (Cisco Firewall Service Module (FWSM) is supported)
CyberGuard	CyberGuard Firewall v4.1, 4.2, 4.3, 5.1
Cyberoam	Cyberoam Firewall Version: 9.5.4
FortiNet	FortiGate Family
Microsoft ISA	Microsoft ISA (firewall,web-proxy, packet filter) Server 2000 & 2004
Secure Computing Sidewinder	Sidewinder G2
Snort	Most versions
SonicWALL	TELE, SOHO, PRO, GX v4.10, 5.x, 6.x
WatchGuard	WatchGuard Firebox Models v5.x, 6.x, 7.x, 8.x, 10.x
Juniper Networks IDP	Juniper Networks IDP Device (version IDP 50)
3Com	3Com X-family devices
IPCop	IPCop Firewall Version 1.4.17 / 1.4.18



If the Firewall device logs contains the time zone information, Firewall Analyzer processes it and normalizes it to time zone of Firewall Analyzer Server

Configuring Check Point Firewalls

Firewall Analyzer supports LEA support for R54 and above and log import from most versions.

Determining the Check Point Version Number

To determine the version number of the Check Point that you are running, use the following command:

```
$FWDIR/bin/fw ver
```

where *\$FWDIR* is the directory where Check Point is installed.

Pre-Requisites

You need to do the following in Smart Dashboard of Check Point Firewall.

Changes in Smart Dashboard :

1. Open the "Smart Dashboard" where all the rules will be displayed. Set the "Track" value as "Account" instead of "log" for all the rules that are allowing the traffic through the Firewall. This can be done by right clicking on "Track" value for each rule and select "Account". When this is set to "Account" the Check Point firewall will log the information regarding bytes.
 2. After setting the "Track" value as "Account" for all the rules, please install all the policies.
-

Virtual Firewall (Virtual Domain) logs

There is no separate configuration required in Firewall Analyzer for receiving logs from Virtual Firewalls of the Check Point physical device.

If **orig_name** attribute is present in the syslog data, then Firewall Analyzer considers that the log source is virtual firewall (vdom). Otherwise the application considers that the log source is physical device. The recognition of logs from the virtual firewall is automatic and no manual configuration is required.

There are two ways of obtaining logs from Check Point firewall:

- Configuring LEA (Log Extraction API) Connection
- Import of Check Point Log Files

The difference between the two ways are:

If you configure LEA connection, the logs will be collected automatically and processed by the Firewall Analyzer. Whereas, if you want import the logs, manual intervention is required. You need to export the syslogs in Check Point Management Station or from Check Point Smart Tracker UI and then manually import the syslog file in Firewall Analyzer.

Configuring LEA Connection

The following instructions will help you set up an authenticated or unauthenticated connection between Firewall Analyzer and the Check Point Management Server. For additional information please refer the Check Point documentation or contact Check Point technical support.

For managing the LEA servers the configurations that needs to be done for the different check point firewalls are explained below:

- Setting up an Unauthenticated LEA Connection
- Setting up an Authenticated LEA Connection

Setting up an Unauthenticated LEA Connection

Follow the steps below to configure an unauthenticated connection from the Check Point Firewall:

Carryout the configuration in the Check Point Firewall Management Station.

1. In the *FWDIR\conf* directory on the computer where the Check Point Management Server is installed, edit the *fwopsec.conf* file to include the following line:
`lea_server port 18184`
`lea_server auth_port 0`
2. Restart the firewall service
`[4.1] fwstop ; fwstart`
`[NG] cpstop ; cpstart`
3. Add a rule to the policy to allow the port defined above `port 18184` (assuming default LEA connection port) from the Firewall Analyzer machine to the Check Point Management Server and vice versa.
4. Install the policy

Adding to LEA Server Lists on Firewall Analyzer

Once this unauthenticated LEA connection has been set up, follow the instructions for Adding an LEA Server to the Firewall Analyzer.

If you are unable to view the Check Point Firewall reports refer the Trouble Shooting Tip.

Setting up an Authenticated LEA Connection

Follow the steps below to configure an authenticated connection from the Check Point Firewall:

Carryout the configuration in the Check Point Firewall Management Station.

1. In the *FWDIR\conf* directory on the computer where the Check Point Management Server is installed, edit the *fwopsec.conf* file to include the following line:

```
lea_server port 0
lea_server auth_port 18184
```

2. Restart the firewall service
[4.1] fwstop ; fwstart
[NG] cpstop ; cpstart
3. Add a rule to the policy to allow the port defined above port 18184 (assuming default LEA connection port) from the Firewall Analyzer machine to the Check Point Management Server and vice versa.
4. Install the policy

The following steps will help you configure an **sslca** authenticated connection to the Check Point firewall, carryout the configuration in the Check Point firewall Management Station:

1. Create a new OPSEC Application Object with the following details:
 - a. Name (e.g., myleaclient)
 - b. Vendor: user defined
 - c. Server Entities: none
 - d. Client Entities: LEA
2. Initialize Secure Internal Communication (SIC) for this OPSEC Application Object and enter the activation key (e.g. def456). Note down this activation key, as you will need it later.
3. Write down the DN of this OPSEC Application Object. This is the Client Distinguished Name, which you need later on.
4. Open the object of the Check Point Management Server and write down the DN of that object. This is the Server Distinguished Name.
5. Add a rule to the policy to allow the port defined above, as well as port 18210/tcp (FW1_ica_pull) in order to allow pulling of PKCS#12 certificate from the Firewall Analyzer to the Check Point Management Server. The port 18210/tcp can be shut down after the communication between Firewall Analyzer and the Check Point Management Server has been established successfully.
6. Install the policy.

Configuring the attributes of Check Point Firewall Server in Firewall Analyzer

OPSEC Application	
Object Name	Ex. myleaclient
Activation Key	Ex. def456
SIC Name	Ex. CN=myleaclient,O=cherry-win1..9mob46
LEA Server	
Authentication Type	Ex. sslca
SIC Name	Ex. cn=cp_mgmt,o=cherry-win1..9mob46

The attributes to be configured are described in the table below:

Attributes	Description
OPSEC Application - Object Name	This is the applications NAME that is defined when creating the application object in the Policy Editor under the OPSEC Applications Properties Name field.
OPSEC Application - Activation Key	This is the one time password (Activation Key) that was defined when clicking 'Communications' in the OPSEC Applications Properties window.

Attributes	Description
OPSEC Application - SIC Name	The SIC name of the OPSEC Application LEA client (the LEA Server on Firewall Analyzer), in the case of authenticated connections.
LEA Server - Authentication Type	The authentication mechanism to be used. The default value is <code>sslca</code> . Supported values in this field are: <code>sslca</code> , <code>sslca_clear</code> , <code>sslca_comp</code> , <code>sslca_rc4</code> , <code>sslca_rc4_comp</code> , <code>asym_sslca</code> , <code>asym_sslca_comp</code> , <code>asym_sslca_rc4</code> , <code>asym_sslca_rc4_comp</code> , <code>ssl</code> , <code>ssl_opsec</code> , <code>ssl_clear</code> , <code>ssl_clear_opsec</code> , <code>fwnl</code> and <code>auth_opsec</code>
LEA Server - SIC Name	The SIC name of the Check Point Management Server.

Importing Check Point Log Files

Before proceeding with the importing of Check Point logs, you need to do the following changes in the Smart View Tracker of the Check Point Firewall to obtain the complete log information:

Changes in Smart View Tracker :


1. Open the "Smart View Tracker" and click on "View" > "Query Properties".
2. Please select the following attributes if they were not selected previously:
 - o Elapsed
 - o Bytes
 - o Client InBound Bytes
 - o Client OutBound Bytes
 - o Server InBound Bytes
 - o Server OutBound Bytes
 - o Status
 - o URL

For Non-LEA connections, there are two ways to create plain text check point log file and export the log file, which then can be imported in Firewall Analyzer. For LEA connections you can skip the below mentioned methods and follow the LEA configuration instructions.

Method 1 :

In the command prompt of Check Point Firewall Management Station execute the following command

```
fw logexport -d ; -i fw.log -o exportresult.log -n
```

	<p>For Check Point NG use the below command:</p> <pre>fwm logexport -d ; -i fw.log -o exportresult.log -n</pre> <p>where, <i>-d</i> refers to <i>delimiter</i>, <i>-i</i> refers to <i>input log file</i>, <i>-o</i> refers to <i>output ASCII file</i>, and <i>-n</i> implies <i>don't perform DNS resolution of the IP addresses in the Log File (this option significantly improves processing speed)</i>.</p>
---	---

For detailed information please refer the Check Point documentation or contact Check Point technical support.

The above command creates an ascii file named *exportresult.log*. Copy or transfer this file to Firewall Analyzer machine. Then in Firewall Analyzer you can Import this log file.

Method 2 :

1. In the Check Point Smart Tracker UI (UI where you are seeing all logs in Check Point Management Station), select All Records option in the left tree.
2. Click "File" > "Export".
3. Give a proper file name, like exportresult.log. Copy or transfer this file to Firewall Analyzer machine. Then in Firewall Analyzer you can Import this log file.

Trouble Shooting Tip

If you are unable to view the Check Point Firewall reports carry out the following procedure:

- Click the Edit/Delete icon of the firewall for which you are unable to view reports. Click **Save**.
- Click the **Enable Debugging Mode** checkbox to enable the Check Point firewall in debugging mode.
- Once saved, create a support information file through Support tab, and send to *fwanalyzer-support@manageengine.com*

Configuring NetScreen Firewall

Firewall Analyzer supports most versions of NetScreen Firewall Appliance (OS 3.x, 4.x, 5.x,...). You can either enable WELF or Syslog format.

Enable Syslog Messages and Disable WebTrends Messages using the NetScreen Administration Tools Console

1. Log in to the NetScreen GUI.
2. Click **Configuration> Report Settings> Syslog** in the left pane of the NetScreen GUI.
3. Select the **Enable Syslog Messages** check box.
4. Select the **Trust Interface as Source IP for VPN** and **Include Traffic Log** check box.
5. Type the IP address of the Firewall Analyzer server and syslog port (514) in the **Syslog Host Name / Port** text box.
6. All other fields will have default values.
7. Click **Apply** to save the changes.
8. Click **Configuration> Report Settings> WebTrends** in the left pane of the NetScreen GUI
9. **Clear** the **Enable WebTrends Messages** check box.
10. Click **Apply** to save the changes.



In certain versions of NetScreen firewall there is an option to record the completion of a transaction. Please select this option (if available) in the NetScreen firewall to enable Firewall Analyzer to measure the sent and received bytes from the firewall traffic logs.



Uncheck the TCP option. This will make the firewall to send syslogs in the configured UDP port.

If you would like to send NetScreen logs in WELF to Firewall Analyzer, the you need to Disable Syslog Messages and Enable WebTrends Messages in the above steps. For more information, refer the NetScreen documentation.

Configure/Enable Syslog Messages for Netscreen Firewall device using CLI Console:

Execute the following commands to configure syslog via CLI:

```
Syngress > set syslog config 10.23.23.2 facilitates local0 local0
Syngress > set syslog config 10.23.23.2 port 514
Syngress > set syslog config 10.23.23.2 log all
Syngress > set syslog enable
```

Configure/Enable WebTrends for Netscreen Firewall device using CLI Console:

Execute the following commands to configure WebTrends via CLI:

```
Syngress > set webtrends host-name 10.23.23.2
Syngress > set webtrends port 514
Syngress > set webtrends enable
```

Configure/Enable SNMP Protocol for Netscreen Firewall device

Using CLI Console:

To add a new SNMP community: (Skip this step, if you have already defined a community)

```
set snmp community "<community name>" Read-Only Trap-off version {any | v1 | v2c}
```

To enable the SNMP Manager running in Firewall Analyzer to make queries to SNMP Agent running in the firewall:

```
set snmp host "<community name>" <Firewall Analyzer IP> [src-interface <interface through which Firewall Analyzer is connected>]
```

Example: The following command example defines the IP address '10.5.1.24' as member of the SNMP community named 'olympia':

```
set snmp host "olympia" 10.5.1.24 [src-interface inside]
```

Enable SNMP manageability on the interface through which the SNMP manager in Firewall Analyzer communicates with the SNMP agent in the NetScreen device.

```
set interface <interface name> manage snmp
```

Using Web UI:

To add a new SNMP community: (Skip this step, if you have already defined a community)

- Log in to the Netscreen web interface
- Go to **Configuration > Report Settings > SNMP > New Community**
- Enter the following settings:
 - **Community Name:** <community name>
 - **Permissions:**
 - **Write:** (select)
 - **Trap:** (clear)
 - **Including Traffic Alarms:** (clear)
 - **Version:** ANY (select)
 - **Hosts IP Address/Netmask and Trap Version:** <Firewall Analyzer IP address>
- Click **Apply**.

To enable the SNMP Manager running in Firewall Analyzer to make queries to SNMP Agent running in the firewall:

- Go to **Configuration > Report Settings > SNMP**

- Edit community to add **SNMP Manager IP** <Firewall Analyzer IP address> and the source interface (interface through which Firewall Analyzer connects firewall) to that community. Under communities section, you will find the option to edit community. If SNMP Agent does not have a community, click '**New Community**' button and provide community string, SNMP Manager IP address <Firewall Analyzer IP address> and the source interface (interface through which Firewall Analyzer connects firewall) to that community.
- Click **Apply**.

Enable SNMP manageability on the interface through which the SNMP manager in Firewall Analyzer, communicates with the SNMP agent in the NetScreen device.

- Go to **Network > Interfaces > Edit (for ethernet1)**
- Enter the following settings:
 - **Service Options:** <no change>
 - **Management Services:** *SNMP*
- Click **OK**.

Configuring Cisco Devices - PIX/ASA/FWSM/VPN Concentrator

Firewall Analyzer supports the following versions of various Cisco devices.

Cisco IOS Firewalls:

- 8xx
- 18xx
- 28xx
- 38xx
- 72xx
- 73xx
- 3005
- 1900
- 2911
- 3925

Cisco FWSM Catalyst Series:

- 6500
- 7600

Cisco PIX versions:

- 6.x
- 7.x

Cisco ASA:

5500 series

Cisco VPN Concentrators Series:

- 3000
- 3500

Model Family	Model	Cisco IOS Software Version
8xx	c871, c876, c877,c878	12.4(4)T
18xx	c1841	12.3(14)T
	c1811, c1812	12.4(4)T
	c1801, c1802, c1803	12.4(4)T
28xx	c2801, c2851, c2821, c2811	12.3(14)T
38xx	c3845, c3825	12.3(14)T
72xx	7206VXR, 7204VXR	12.3(14)T
73xx	CISCO7301	12.3(14)T

To find out the version of your PIX firewall, Telnet to the PIX firewall and enter the show version command.



Cisco PIX does not create log files, but instead directs a log stream to the syslog server, which writes the log information into a file. Make sure the syslog server on Firewall Analyzer can access the PIX firewall on the configured syslog port. For this, you may have to make a rule specific to this situation.

- Getting logs from Virtual Firewall (Virtual Domain)
- Configuring Cisco PIX using Command Line Interface
- Configuring Cisco PIX from the User Interface
- Configuring SNMP protocol for Cisco PIX using Command Line Interface
- Configuring Cisco ASA using Command Line Interface
- Configuring SSL WebVPN in Cisco ASA appliance
- Configuring Cisco ASA NetFlow Logs
- Configuring SNMP protocol for Cisco ASA using Command Line Interface
- Configuring Cisco VPN 3000 Concentrator
- Configuring Cisco IOS Switch
- Configuring SNMP protocol for Cisco Firewalls using ASDM Web UI tool

Virtual Firewall (Virtual Domain) logs

Prerequisite for context/vdom in Cisco Firewalls

The Cisco Firewall IP address should be DNS resolvable from Firewall Analyzer.

There is no separate configuration required in Firewall Analyzer for receiving logs from Virtual Firewalls of the Cisco physical device.



Configuration in Cisco device for Virtual Firewall

In order to support virtual firewalls for Cisco devices, you need to enable logging based on the **context-name**. Otherwise it is not possible for Firewall Analyzer to detect Virtual Firewalls (vdom) of Cisco devices.

Configuring Cisco PIX using Command Line Interface

1. Telnet to the PIX firewall and enter the enable mode
2. Type the following:


```
configure terminal
logging on
logging timestamp
logging trap informational
logging device-id {context-name | hostname | ipaddress interface_name
| string text}
logging host interface_name syslog_ip [17/<syslog_port>]
```

where,

interface_name	is the interface on the PIX firewall whose logs need to be analyzed ("inside" or "outside," for example).
syslog_ip	is the IP address of the syslog server (i.e. Firewall Analyzer), to which the Firewall should send the Syslogs.
17/<syslog_port>	indicates that logs will be sent using the UDP protocol, to the configured syslog port on the syslog server. If left blank, the syslogs are sent through the default syslog port (UDP port 514). If the logs are sent through any other port, mention it as 17/<the UDP port number> (For example: 17/1514).
hostname	firewall's host name (defined with the hostname configuration command). In this case, the hostname will appear in the logs sent from the Firewall.
ipaddress interface_name	the IP address of a specific firewall interface named interface_name ("inside" or "outside," for example). In this case, the IP Address of the Interface Name will appear in the logs sent from the Firewall.
string text	an arbitrary <i>text</i> string (up to 16 characters). In this case, the arbitrary text string you have entered in string <text> will appear in the logs sent from the Firewall.
context-name	in PIX 7.x or FWSM 2.x operating in multiple-context mode, the name of the firewall context will appear in the logs sent from the Firewall.

Example: logging host inside 11.23.4.56 17/1514

To verify your configuration, enter the `show logging` command after the last command above. This will list the current logging configuration on the PIX firewall.

Configuring Cisco PIX from the User Interface

Log in to the Cisco PIX user interface, and follow the steps below to configure the PIX firewall:

1. *Enabling Logging*
 - a. Select **Configure > Settings > Logging > Logging Setup**
 - b. Select the **Enable logging setup** and **Enable logging failover** check boxes
 - c. Click **Apply**.
Changes are applied to the assigned PIX firewall configuration files when they are generated. The configuration files are then downloaded to PIX firewalls at deployment.
2. *Configuring Syslog Server*
 - a. Select **Configure > Settings > Logging > Syslog**
 - b. Check **Include Timestamp**.
 - c. Click **Add** to add a row.
 - d. In the **Add Syslog Server** page that appears, enter the following:
 - i. **Interface Name** - the firewall interface through which Firewall Analyzer can be reached, the interface can be either inside or outside.

- ii. **IP Address** - the IP address of the syslog server to which logs have to be sent
- iii. Under **Protocol**, select the **UDP** radio button
- iv. The default UDP port is 514. If you have configured a different syslog listener port on your syslog server, enter the same port here.
- e. Click **Apply**
- 3. *Configuring Logging Level*
 - a. Select **Configure > Settings > Logging > Other**
 - b. Under **Console Level List** select **Informational** so that all report data is available
 - c. Click **Apply**

Configure/Enable SNMP Protocol for Cisco PIX Firewall device

Using CLI Console:

To enable the SNMP Manager running in Firewall Analyzer to make queries to SNMP Agent running in the firewall:

```
configure terminal
snmp-server host <interface name> <hostname | IP address of Firewall Analyzer>
```

If you want to create a new SNMP community use the below command:

```
configure terminal
snmp-server community <community-string>
```

Example:

```
configure terminal
snmp-server community public
```

Configuring Cisco ASA Versions

1. Telnet to the ASA firewall and enter the enable mode
2. Type the following:

```
configure terminal
logging enable
logging timestamp
logging trap informational
logging device-id {context-name | hostname | ipaddress
interface_name | string text}
logging host interface_name syslog_ip [udp/<syslog_port>]
```

3. If there are no URL Reports available in Firewall Analyzer for CISCO ASA, enable HTTP inspection by executing the following command:
- ```
inspect http
```

Enabling HTTP inspection will generate syslogs with ID 304001. This ID will be used by Firewall Analyzer to generate URL Reports.

|                             |                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface_name              | is the interface on the ASA Firewall whose logs need to be analyzed (for example: "inside" or "outside").                                                                  |
| syslog_ip                   | is the IP address of the syslog server (i.e. Firewall Analyzer), to which the Firewall should send the Syslogs.                                                            |
| udp/<syslog_port>           | indicates that logs will be sent using the UDP protocol, to the configured syslog port on the syslog server. If left blank, logs will be sent to the default UDP port 514. |
| hostname                    | firewall's host name (defined with the <b>hostname</b> configuration command)                                                                                              |
| ipaddress<br>interface_name | the IP address of a specific firewall interface named interface_name (for example: "inside" or "outside")                                                                  |
| string text                 | an arbitrary text string (up to 16 characters)                                                                                                                             |
| context-name                | in PIX 7.x or FWSM 2.x operating in multiple-context mode, the name of the firewall context can also be sent.                                                              |

For more information, refer the Cisco PIX documentation.

## Configuring Cisco ASA Versions using ASDM

### Enable Logging

Carry out the steps given below:

- Load the **ASDM**
- Select Configuration > Device Management > Logging > Logging Setup
- Select Enable Logging
- Select Logging > Logging Filters
- Choose the syslog-servers as **Informational**
- Select Logging > Logging Filters > Syslog servers
- Click **Add**
- Enter the IP address and choose the appropriate interface and ensure that you choose UDP and enter the port number
- Select Logging > Syslog Setup
- Select 'Include time stamp in syslogs' option and scroll down to ensure the syslog ID's 302013, 302014, 302015, 302016 are in enabled state and the logging level is set to **Informational**

### Disable Logging

You can disable specific syslog IDs based on your requirement.

**Note:** By selecting the check mark for the Include timestamp in syslogs option, you can add the date and time that they were generated as a field to the syslogs.

- Select the syslogs to disable and click **Edit**.
- From the **Edit Syslog ID Settings** window, select the **Disable** messages option and click **OK**.
- The disabled syslogs can be viewed in a separate tab by selecting **Disabled syslog IDs** from the **Syslog ID Setup** drop-down menu.

For more information, refer the Cisco PIX documentation.

## Configuration for SSL WebVPN in Cisco ASA appliance

Firewall Analyzer requires syslog message IDs 722030 and 722031, which by default is at debug level, to process Cisco SVC VPN logs. Set the information level to these syslog IDs by executing below commands in global configuration mode:

```
hostname(config)# logging message 722030 level 6
hostname(config)# logging message 722031 level 6
```

You can confirm by executing the below command:

```
hostname(config)# show logging message 722030
```

## Configuring Cisco ASA NetFlow Logs and Disabling NetFlow on Cisco ASA/ADM using command line and ASDM

Firewall Analyzer support **NetFlow version 9** packets, which is introduced in **Cisco ASA 8.2.1/ASDM 6.2.1**.

Configuring ASA device using console mode to send NetFlow version 9 packets to Firewall Analyzer is given below:

- As Firewall Analyzer is capable of receiving either Syslog or NetFlow packet from an ASA box, disable Syslog and enable NetFlow.

To disable Syslog and enable NetFlow execute the following commands:

```
(config)# flow-export destination inside <Firewall Analyzer Server IP>
1514
(config)# flow-export template timeout-rate 1
(config)# flow-export delay flow-create 60
(config)# logging flow-export-syslogs disable ---> This command will
disable logging syslog messages
(config)# access-list netflow-export extended permit ip any any
(config)# class-map netflow-export-class
(config-cmap)#match access-list netflow-export
```

## Associate global policy map with netflow class map

### Option 1

If you have a global policy map, associate the above netflow class-map **netflow-export-class** to the global policy.  
For example: if your global policy map is named **global\_policy\_asa**, you need to execute the below commands:

```
(config)# policy-map global_policy_asa
(config-pmap)# class netflow-export-class
(config-pmap-c)# flow-export event-type any destination <Firewall
Analyzer Server IP>
if the above command fails use the below:
```

```
(config-pmap-c)# flow-export event-type all destination <Firewall
Analyzer Server IP>
```

- **Option 2**

If you wish to create a new policy map named **netflow-export-policy** and make this as your global policy follow the below steps:

```
(config)# policy-map netflow-export-policy
(config-pmap)# class netflow-export-class
(config-pmap-c)# flow-export event-type any destination <Firewall
Analyzer Server IP>
```

if the above command fails use the one below:

```
(config-pmap-c)# flow-export event-type all destination <Firewall
Analyzer Server IP>
```

Make policy map **netflow-export-policy** as your global policy:

```
(config)# service-policy netflow-export-policy global
```

For UI mode configuration using ASDM access, refer the Cisco forum topic:  
<https://supportforums.cisco.com/docs/DOC-6114>

**To disable NetFlow on Cisco ASA/ADM execute the following commands:**

```
(config)# flow-export disable
(config)# no flow-export destination inside <Firewall Analyzer Server IP>
1514
```

**To disable NetFlow on Cisco ASA/ADM using ASDM**

- Click on Configuration > Firewall
- Click on Service Policy Rules. Look for the policy indicating netflow export
- Check the IP address if the flow is pointing to the machine where you want to forward syslog.
- If so, delete it and write the configuration in to memory (Save it).

**Configure/Enable SNMP Protocol for Cisco ASA Firewall device**

**Using CLI Console:**

To enable the SNMP Manager running in Firewall Analyzer to make queries to SNMP Agent running in the firewall:

```
configure terminal
snmp-server enable
snmp-server host <interface name> <hostname | IP address of Firewall Analyzer>
[poll]
```

**Example:**

```
configure terminal
snmp-server enable
snmp-server host inside 192.168.101.155 poll
```

If you want to create a new SNMP community use the below command:

```
configure terminal
snmp-server community <community-string>
```

**Example:**

```
configure terminal
snmp-server community public
```

### Configuring Cisco VPN 3000 Concentrator

Currently we support **Cisco IOS Compatible** Log Format and **Original Log** Format for Cisco VPN Concentrator.

Importing of already saved Cisco VPN Concentrator logs is not supported because those logs are saved in either of the following formats which is **not supported** in Firewall Analyzer:

- Multi line
- Tab Delimited
- Comma Delimited

Follow the below steps to configure the VPN Concentrator:

1. *Configuring Syslog Server*
  - a. Login to the Cisco VPN 3000 Concentrator Management console.
  - b. Go to **Configuration > System > Events > Syslog Servers**
  - c. Click the **Add** button
  - d. In the **Syslog Server** text box enter the IP Address of the machine where Firewall Analyzer is running.
  - e. Enter the **Port** value. The default syslog server port for Firewall Analyzer is 514.
  - f. Facility is **Local 7**
2. *Configuring Syslog Events*
  - a. Go to **Configuration > System > Events > General**
  - b. For **Syslog Format** you can either select **Original** or **Cisco IOS Compatible** format.
  - c. For **Events to Syslog** select **Severities 1-5**
  - d. All other configurations are default for this page.
  - e. Click **Apply** button

For more information, refer the Cisco VPN Concentrator documentation.

### Configuring Cisco IOS Switch

Follow the below steps to configure the Cisco IOS Switch:

1. Login to the Cisco IOS console or Telnet to the device.
2. Change the configuration mode of the device.



Use the following command:

```
configure terminal
```

3. Enable logging by using the following commands:

```
logging on
logging trap informational
logging <IP Address>
```

4. If there is a Firewall module in the IOS device, use the following command to enable audit trail. This will generate traffic information.

```
ip inspect audit-trail
```

For more information, refer the Cisco IOS Switch documentation.

### Configure/Enable SNMP Protocol for Cisco Firewall devices using Cisco ASDM tool

#### Using Web UI:

#### Configure SNMP parameters for SNMP Versions 1 and 2c

Carry out the following steps:

- In the **ASDM** main window, select **Configuration > Device Management > Management Access > SNMP**
- In the **Community String** (default) field, enter default community string. This applies to SNMP Versions 1 and 2c only
- Fill appropriate values in **Contact** and **Location** fields
- In the **Listening Port** field, enter the port number of the security appliance that listens for SNMP requests from management stations; or retain the default port number **161**
- Click **Apply**

With this, SNMP parameters for Versions 1 and 2c are configured and the changes are saved to the running configuration.

To enable the SNMP Manager running in Firewall Analyzer to make queries to SNMP Agent running in the firewall:

- In the **ASDM** main window, choose **Configuration > Device Management > Management Access > SNMP**
- In the **SNMP Management Stations** pane, click **Add**. The **Add SNMP Host Access Entry** dialog box appears
- In the **Interface Name** drop-down list, choose the interface on which the Firewall Analyzer resides
- In the **IP Address** field, enter the Firewall Analyzer IP address
- In the **UDP Port** field, enter the Firewall Analyzer UDP port, or retain the default port **162**
- In the **Community String** field, enter the Firewall Analyzer community string. If no community string is specified for a management station, the

value set in the **Community String** (default) field on the SNMP Management Stations pane is used

- In the **SNMP Version** drop-down list, choose the SNMP version used by the Firewall Analyzer
- If you have selected **SNMP Version 3** in the previous step, in the **Username** drop-down list, choose the name of a configured user
- To specify the method for communicating with this management station, check the **Poll** check boxes
- Click **OK**. The **Add Firewall Analyzer Access Entry** dialog box closes.
- Click **Apply**.

With this, the management station is configured and changes are saved to the running configuration.

### Configure SNMP Parameters for Version 3:

SNMP Version 3 allows you to configure additional authentication and privacy options for more secure protocol operations by means of SNMP server groups and users.

Carry out the following steps:

- In the **ASDM** main window, choose **Configuration > Device Management > Management Access > SNMP**
- In the **SNMPv3 Users** pane, to add a configured user or a new user to a group, click **Add**. To change user parameters, click **Edit**. To remove a configured user from a group, click **Delete**. When you remove the last user in a group, **ASDM** deletes the group



**Note:** Once a user is created, you cannot change the group to which the user belongs.

- The **Add SNMP User Entry** dialog box appears
- In the **Group Name** drop-down list, choose the group to which the SNMP user will belong. The available groups are as follows:
  - **Auth&Encryption**, in which users have authentication and encryption configured
  - **Authentication\_Only**, in which users have only authentication configured
  - **No\_Authentication**, in which users have neither authentication nor encryption configured
- In the **Username** field, enter the name of configured user or new user. The username must be unique for the SNMP server group selected
- To have the password encrypted, click the **Encrypt Password** radio button. If you choose this option, you must enter the password as **MD5** hash value.
- Indicate the type of authentication you want to use by clicking the appropriate radio button: **MD5** or **SHA**
- In the **Authentication Password** field, type the password to use for authentication
- Indicate the type of encryption you want to use by clicking the appropriate radio button: **DES** or **3DES**, or **AES**
- If you chose **AES** encryption, from the **AES Size** drop-down list, specify which level of **AES** encryption to use: **128** or **192** or **256**
- In the **Encryption Password** field, type the password to use for encryption. The maximum number of characters allowed for this password is **64**

- Click **OK** to create a group (if this is the first user in that group), display this group in the **Group Name** drop-down list, and create a user for that group. The **Add SNMP User Entry** dialog box closes
- The **SNMPv3 Users** pane lists the following information: **SNMP Version 3** server group name, name of the user that belongs to the specified group, encrypted password setting, authentication setting, encryption algorithm setting, and the **AES** size setting
- Click **Apply**

With this, SNMP parameters for Version 3 are configured, and the changes are saved to the running configuration.

## Configuring Microsoft ISA Server

Firewall Analyzer supports Microsoft Internet Security and Acceleration (ISA) Server 2000, 2004, & 2006.

### Supported ISA Log Formats in Firewall Analyzer:



Firewall Analyzer supports **W3C extended log file format** for *Packet filters, ISA Server Firewall Service, and ISA Server Web Proxy Service*. **ISA Server File log format** is supported for *ISA Server Web Proxy Service* only.

### Configuring Microsoft ISA Server

1. Open the "ISA Management" console.
2. Select "Monitoring Configuration" from the left-hand side console tree, and then select the "Logs" folder.
3. In the "Logs" folder, right click on each of the listed component (like *Packet filters, ISA Server Firewall Service, ISA Server Web Proxy Service*), select "Properties" and set the log format to **W3C extended log file format**.

For more information, refer the Microsoft ISA Server documentation.

Once you have configured the ISA Server, then in Firewall Analyzer you can Import this log file.

- You can schedule the import of logs using localhost. You can share the ISA log folder and can map it to network drive of Firewall Analyzer server. Then, you can schedule the local import to import periodically.  
In case if you are running Firewall Analyzer as a service, you should ensure that Firewall Analyzer has enough permission to access the file in shared folder.
- If you want Firewall Analyzer to periodically import the ISA Server logs use FTP import provision in "Remote Host", with the time interval less than the time interval set in the ISA Server.



We recommend Local Import Schedule option over Remote Host FTP Import option.

Firewall Analyzer handles Dynamic Filename change of ISA Server log files.



Microsoft ISA Proxy server creates log file with new name (with time stamp appended) everyday. If the Microsoft ISA Proxy log files are to be imported, you do not have to change the filename daily, instead select the **Change filename dynamically** option while importing the logs. Selecting the option displays the **Filename pattern:** text box to enter the time stamp pattern that the Proxy server appends when the Proxy server creates the log file daily. A help tip icon displays, (when you hover the mouse on the icon) the mapping of the *Timestamp in Filename* to the *Pattern to be given*. Enter the pattern as required.

## Configuring Microsoft ISA Server 2004 & 2006

By default Microsoft ISA Server 2004 & 2006 stores log files into MSDE databases (Microsoft SQL Desktop Engine).

### Log files options placement in ISA Management Console 2004 & 2006

In order to switch log files format from MSDE to W3C please do the following:

- Run ISA Management Console
- Select **Monitoring** item on the left pane
- Select **Logging** tab on the center pane
- Select **Tasks** tab on the right pane

You will need to change log files format for Firewall and Web proxy. Please choose **Configure Firewall Logging** and **Configure Web Proxy Logging** items and perform actions shown below for each.

### Log file format settings for Firewall and Web Proxy

Check on File option. In the dropdown list select **W3C extended log file format**. **Enable logging for this service** option should be enabled. If you want to change log files location, press **Options** button, another dialog will appear where you can change the log files path, **Compress log files** and **Delete log files** older than should remain disabled. Select **Fields** tab and check that all necessary fields are enabled. Please see table below for the list of necessary fields.

#### Necessary Fields

| Firewall log files      | Web proxy log files |
|-------------------------|---------------------|
| Log Date                | Client IP           |
| Log Time                | Client Username     |
| Transport               | Client Agent        |
| Client IP and port      | Log Date            |
| Destination IP and port | Log Time            |
| Action                  | Bytes Received      |
| Protocol                | Bytes Sent          |
| Bytes sent              | Protocol            |
| Bytes sent Delta        | URL                 |
| Bytes received          | Object source       |
| Bytes received Delta    | HTTP Status Code    |
| Client Username         |                     |
| Client Agent            |                     |

ProxyInspector work only with log files since access to the log files is significantly faster than access to SQL databases (nevertheless you can import data from existing MSDE databases using **Database | Move data from ISA 2004 & 2006 MSDE databases**). ProxyInspector supports both W3C and ISA Native log files formats. Recommended format is W3C.

## Configuring CyberGuard

---

Firewall Analyzer supports CyberGuard Firewall v4.1, 4.2, 4.3, 5.1

### Configuring CyberGuard

On the Cyberguard Firewall Configuration console do the following.

1. Click **Configuration** and select **Alerts and Activities**.
2. Select **Activity Reports** in WebTrends format to send it via syslog.
3. Select facility and severity.
4. Type the Firewall Analyzer IP to which CyberGuard should write the syslog information.

You can select WebTrends log format for Audit logs too. Either you can send the syslogs to the default listener ports (514 or 1514) of Firewall Analyzer or you can import the text log file into Firewall Analyzer.



In case, if Firewall Analyzer shows "Unknown Packet Received", send the sample logs present under <FirewallAnalyzerHome>/server/default/archive/<firewallip> directory, to fwanalyzer-support@manageengine.com for us to troubleshoot.

## Configuring Cyberoam

Firewall Analyzer supports Cyberoam Firewall Version: 9.5.4 build 66 onwards

### Configuring Cyberoam

On the Cyberoam Firewall Web Admin Console do the following.

1. Select **System > Logging > Manage Syslog**
2. Specify unique name for **Syslog server**
3. Specify **IP address** and **port** of the syslog server. Cyberoam will send logs to the configured IP address. The default port is 514
4. Select **Facility**. Facility indicates the source of a log message to the syslog server. You can configure **Facility** to distinguish log messages from different Cyberoam Firewalls
5. Select the **Severity** level of the messages logged. Severity level is the severity of the message that has been generated



Cyberoam logs all messages at and above the logging severity level you select. For example, select ?ERROR? to log all messages tagged as ?ERROR,? as well as any messages tagged with ?CRITICAL,? ?ALERT? and ?EMERGENCY? and select ?DEBUG? to log all messages.

**Note:** Firewall Analyzer requires the severity level as 'INFORMATIONAL'.

6. Click **Create** to save the configuration.

Also you need to enable logging on each rule to monitor allowed and denied traffic. Please follow the below steps.

- Click **Log Traffic** to enable/disable traffic logging for the rule. Ensure firewall rule logging is in **On/Enable** state in the Logging Management. Refer to Cyberoam Console Guide, Cyberoam Management for more details.
- To log the traffic permitted and denied by the firewall rule, you need to keep **On/Enable** state in the firewall rule logging from the **Web Admin Console > Firewall rule and from the Telnet Console > Cyberoam Management**.
- Specify full description of the rule, displays full description of the rule, modify if required.

| Matching Criteria                                                                                                                                                  |                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Id                                                                                                                                                           | General                                                                                                                                                         |
| Source *                                                                                                                                                           | LAN                                                                                                                                                             |
| <input checked="" type="checkbox"/> Check Identity                                                                                                                 | Any Live User                                                                                                                                                   |
| Destination *                                                                                                                                                      | WAN                                                                                                                                                             |
| Service/Service Group*                                                                                                                                             | All Services                                                                                                                                                    |
| Apply Schedule                                                                                                                                                     | All the Time                                                                                                                                                    |
| Firewall Action When Criteria Match                                                                                                                                |                                                                                                                                                                 |
| Action*                                                                                                                                                            | Accept                                                                                                                                                          |
| <input checked="" type="checkbox"/> Apply Source NAT                                                                                                               | MASQ                                                                                                                                                            |
| <input type="checkbox"/> Advanced Settings (Destination NAT, IDP Policy, Internet Access Policy, Bandwidth Policy, Anti-Virus and Anti-Spam Settings, Log Traffic) |                                                                                                                                                                 |
| Policies                                                                                                                                                           |                                                                                                                                                                 |
| IDP Policy                                                                                                                                                         | Select Here                                                                                                                                                     |
| Internet Access Policy                                                                                                                                             | Select Here                                                                                                                                                     |
| Bandwidth Policy                                                                                                                                                   | Select Here                                                                                                                                                     |
| Anti-Virus & Anti-Spam Settings                                                                                                                                    |                                                                                                                                                                 |
| Scan Protocol(s)                                                                                                                                                   | <input type="checkbox"/> SMTP <input type="checkbox"/> POP3 <input type="checkbox"/> IMAP <input type="checkbox"/> FTP <input checked="" type="checkbox"/> HTTP |
| Log Traffic                                                                                                                                                        |                                                                                                                                                                 |
| Log Traffic                                                                                                                                                        | <input type="checkbox"/> Enable                                                                                                                                 |

- Click **Save** to save the rule.



## Configuring Fortinet Firewalls

Firewall Analyzer supports the following versions of FortiGate:

- FortiOS v2.5, 2.8, and 3.0
- Fortinet - 50, 100, 200, 300, 400, 800
- Fortigate - 1000, 5000 series



Firmware v2.26 or later is required

### Prerequisite to get Application report

Information about Applications like Skype, FaceBook, YouTube and application categories accessed by users will be available in this report. This report is available for Fortigate only. Ensure Application Control service in their Fortigate firewall is enabled to generate the Application report.

### Virtual Firewall (Virtual Domain) logs

There is no separate configuration required in Firewall Analyzer for receiving logs from Virtual Firewalls of the Fortinet physical device. For configuring High Availability for FortiGate Firewall with vdoms, refer the procedure given below.

### Prerequisite to support vdom

In order to get the vdom support for Fortigate Firewall, ensure that the log format selected is Syslog instead of WELF.

If Firewall Analyzer is unable to receive the logs from the Fortigate after configuring from UI, please carryout the steps to configure it through command prompt

To determine the version number of the Fortigate that you are running, use the command: *get system status*

### Configuring the FortiGate Firewall

Follow the steps below to configure the FortiGate firewall:

1. Log in to the FortiGate web interface
2. Select **Log & Report > Log Setting** or **Log & Report > Log Config > Log Setting** (depending on the version of FortiGate)
3. If you want to export logs in WELF format:
  - o Select the **Log in WebTrends Enhanced Log Format** or the **WebTrends** checkbox (depending on the version of FortiGate)
  - o Enter the IP address of the syslog server

- Choose the logging level as **Information** or select the **Log All Events** checkbox (depending on the version of FortiGate)
- 4. If you want to export logs in the syslog format (or export logs to a different configured port):
  - Select the **Log to Remote Host** option or **Syslog** checkbox (depending on the version of FortiGate) Syslog format is preferred over WELF, in order to support vdom in Fortigate firewalls.
  - Enter the IP address and port of the syslog server
  - Select the logging level as **Information** or select the **Log All Events** checkbox (depending on the version of FortiGate)
  - Select the facility as **local7**
- 5. Click **Apply**



Do not select **CSV format** for exporting the logs.

### Configuring RuleSets for Logging Traffic

Follow the steps below to configure rulesets for logging all traffic from or to the FortiGate firewall:

1. Select **Firewall > Policy**
2. Choose a rule for which you want to log traffic and click **Edit**. You can configure any traffic to be logged separately if it is acted upon by a specific rule.
3. Select the **Log Traffic** checkbox
4. Click **OK** and then click **Apply**

Repeat the above steps for all rules for which you want to log traffic.  
For more information, refer the Fortinet documentation.

**If Firewall Analyzer is unable to receive the logs from the Fortigate after configuring from UI, please carryout the steps to configure it through command prompt**

(For the models like Fortigate 60, Fortigate 200, etc.)

Please follow the steps to enable the device to send the logs to Firewall Analyzer.

- Start CLI on the Fortigate firewall.
- Execute the following commands to enable Syslog:

```
Enable syslog:
config log syslogd setting<cr>
set server (ip address)<cr>
set status enable<cr>
end<cr>
```

- Execute the following commands to enable Traffic:

```
Enable traffic:
config log syslogd filter<cr>
set severity information<cr>
```

```

set traffic enable<cr>
set web enable<cr>
set email enable<cr>
set attack enable<cr>
set im enable<cr>
set virus enable<cr>
end <cr>

```



Type "show log syslogd filter" to list all available traffic.

- Stop and start the Firewall Analyzer application/service and check if you are able to receive the Fortigate Firewall packets in Firewall Analyzer.

### Configure/Enable SNMP Protocol for Fortigate Firewall device

#### Using CLI Console:

Ensure SNMP is enabled in Fortigate box by using the below command:

```
get system snmp sysinfo
```

If it is disabled, enable it by using the below commands:

```

config system snmp sysinfo
set status enable
end

```

To enable the SNMP Manager running in Firewall Analyzer to make queries to SNMP Agent running in the firewall:

```

config system snmp
edit <SNMP Community ID>
config hosts
edit <SNMP Community ID>
set interface <Interface through which Firewall Analyzer is connected to Firewall>
set ip <Firewall Analyzer machine IP address>
end
end

```

To ensure the source interface that connects Firewall Analyzer to Firewall device allows SNMP traffic, execute the below command:

```
get system interface <interface name>
```

To allow SNMP traffic through the source interface use the below command:


```

config system interface internal
set allowaccess <proto1 proto2 SNMP>
end

```

**Using Web UI :**

- Log in to the FortiGate web interface
- Go to **System > Config > SNMP v1/v2c**
- Select **Enable** for the SNMP Agent
- Enter **Description**, **Location** and **Contact** information.
- Click **Apply**.

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• If you already have a SNMP community, edit it to provide Firewall Analyzer (SNMP Manager) IP address. Also specify the source interface through which Firewall Analyzer connects to Firewall.</li> <li>• If you want to add a new SNMP community, click '<b>Create New</b>' button and enter <b>Community Name</b>. Provide Firewall Analyzer (SNMP Manager) IP address and the source interface through which Firewall Analyzer connects to Firewall.</li> </ul> |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**To activate SNMP traffic in the source interface:**

- Go to **System > Network > Interface**.
- For the interface allowing SNMP traffic, select **Edit**.
- Select **SNMP** for **Administrative Access**.
- Select **OK**.

**Configure Fortigate in High Availability Mode:**

In case of Fortigate Firewalls , **device\_id** is considered as resource name in Firewall Analyzer. In the High Availability mode, eventhough both active and standby Firewalls have the same name, the **device\_id** will be different. So, Firewall Analyzer displays them as two devices. To avoid this, you can configure the device name (*devname*) of standby Firewall as **device\_id** of active Firewall. Syslogs from the FortiGate Firewall will transmit the serial number of the device as the value of device\_id field and the host name as the value of the device name (devname) field.

**Example:**

**Active Firewall log:** <189>date=2011-09-28 time=13:14:58 devname=DSAC456Z4  
device\_id=FGT80G3419623587 log\_id=0021000002

**Standby Firewall log:** <188>date=2011-09-28 time=13:14:59  
devname=FGT80G3419623587 device\_id=FGT80G4534717432 log\_id=0022000003

## Configuring WatchGuard Firebox

Firewall Analyzer supports both **WELF** and **native** log formats of WatchGuard Firebox Models v 5.x, 6.x, 7.x, 8.x, 10.x, 11, Firebox X series, x550e, x10e, x1000, x750e



For 8.x version, the XML log file format can be imported by Firewall Analyzer.

### Virus reports are supported only for WatchGuard v10.x

For analysing native logs, the configuration is straight forward, you just need to forward the native logs from WatchGuard to the syslog listener ports of Firewall Analyzer.

By default, WatchGuard Firewall logs do not contain the bytes nformation. It just has the size of the packet and header. So one needs to do the following to enable them,

- For version 7.3 , you need to go into **General Setting** area of your proxy and select the check box **Send log message with summary of each transaction**.
- For version 7.2.1, you need to select the check box **Log accounting/auditing information** in your proxy service.
- For version 8.x , you need to select the check box **Send a log message with summary information for each transaction** in your proxy service.
- For version 10.X,
  - For External and VPN interface based logging:
    - Open **Policy Manager**.
    - Select the **Setup > Logging > Performance Statistics** menu, enable check box and save configuration.
  - For proxy level tracking:
    - Edit the proxy action and select the check box **Turn on logging for reports** for each desired proxy and save configuration



Device configuration for Firebox X1250e, XTM 11 series

#### Bytes Information for Watch Guard:

Please follow the steps and configure the same in the Watchguard device to resolve the issue.

- Ensure that your Watch Guard policies are created with Proxy Action and then follow the steps
- Action > Proxies and add the new policy as per your requirement

Please follow the Steps to enable bytes information in the logs:

#### For External and VPN interface based logging:

Setup > Logging > Performance Statistics. Enable check box and save configuration.

For proxy level tracking, edit the proxy action and select '**Turn on logging for reports**' for each desired proxy and save configuration.

|                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Please refer the link of the forum post reply for your reference.<br/><a href="http://www.watchguard.com/forum/default.asp?action=9&amp;boardid=2&amp;read=19115&amp;fid=43">http://www.watchguard.com/forum/default.asp?action=9&amp;boardid=2&amp;read=19115&amp;fid=43</a></p> <p>Please refer WatchGuard website/WatchGuard forums for detailed information.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

You can also configure WatchGuard to export the logs in WebTrends Enhanced Log File (WELF) format, refer WatchGuard documentation for configuring WELF format in WatchGuard Firewalls. Once the log has been exported to WELF format, login to Firewall Analyzer UI and click **Settings > Imported Log Files > Import Log File** option to load the file.

## Configuring Snort

---

Firewall Analyzer supports most versions of Snort.

### Configuring Snort

1. Shutdown the Snort server, if it is running.
2. Login as *root* if you installed Snort in Linux machine.
3. In **snort.conf** file (available at **/etc/snort/snort.conf** in linux and **c:\Snort\bin\snort.conf** in windows) uncomment the line that contains **output information\_syslog** and enter the logging facility and the desired detail level (for example: **output alert\_syslog:host=hostname:port, LOG\_AUTH LOG\_ALERT**)
4. Add the line **config show\_year** to ensure that year has been included in the alerts generated by Snort.
5. Save and exit the **snort.conf** file.
6. In Linux(only) edit the **syslog.conf** file in the **/etc** directory.
7. Append **\*. \* @<server\_name>** at the end, where **<server\_name>** is the name of the machine on which Firewall Analyzer is running.
8. Save the configuration and exit the editor.
9. Restart the syslog service on the host using the command:  
**/etc/rc.d/init.d/syslog restart**
10. Restart the Snort server with **-M** option.

## Configuring Secure Computing Sidewinder

---

Firewall Analyzer supports Sidewinder G2.

### Configuring Sidewinder To Send Audit Data To Firewall Analyzer

1. Open `/etc/sidewinder/auditd.conf`
2. Add the following line at the end of the file, to configure syslog to use the Sidewinder Export Format (SEF):  
`syslog (local0 filters["NULL"] sef)`

You can use 'local0' through 'local7' as names for the facility; they are predefined in syslogd.

3. Save the configuration and exit the editor.
4. Open `/etc/syslog.conf`
5. Append `local0.* @<server_name>` at the end, where facility `local0` matches the facility mentioned in step 2 and `<server_name>` is the name of the machine where Firewall Analyzer is running.
6. Save the configuration and exit the editor.
7. Look up syslog's process ID by entering the following command:  
`pss syslog`
8. Implement the changes by restarting the syslogd and auditd processes, using the following two commands:  
`kill -HUP <syslog process ID>`  
`cf server restart auditd`

The Sidewinder G2 will now send audit data to Firewall Analyzer.



## Configuring SonicWALL Internet Security Appliances

---

Firewall Analyzer supports most of the versions of SonicWALL Firewall devices.

### Configuring SonicWALL To Direct Log Streams

1. Log in to the SonicWALL appliance
2. Click **Log** on the left side of the browser window
3. Select the **Log Settings** tab
4. Type the IP address of the Firewall Analyzer server in the **Syslog Server** text box
5. Click **Update** at the bottom of the browser window

### Configuring SonicWALL Logging Level

1. Log in to the SonicWALL appliance
2. Click **Log** on the left side of the browser window
3. Select the **View** tab
4. Select the **Logging Level** as *Informational* from the combo box
5. Click **Update** at the bottom of the browser window

For more information, refer the SonicWALL documentation in the URL given below:  
[http://help.mysonicwall.com/sw/jpn/2907/ui2/42600/Help/42\\_Log\\_Reporting.html](http://help.mysonicwall.com/sw/jpn/2907/ui2/42600/Help/42_Log_Reporting.html)

Whenever you create an access rule in the SonicWALL Firewall, ensure that '**Enable Logging**' check box is selected for the particular rule. For more information refer the URL <http://www.techrepublic.com/article/how-do-i-configure-firewall-security-on-a-sonicwall-device/6124340>

- Restart the SonicWALL appliance for the changes to take effect.

### To get Live reports using Syslog

Enable 'default' (syslog) format in the SonicWALL firewall to get live reports using syslog

## Configuring Juniper Devices

Firewall Analyzer supports the following Juniper devices.

- Juniper SRX Device (version SRX100, SRX210, SRX220, SRX240, SRX650, SRX1400, SRX3400, SRX3600, SRX5600, SRX5800)
- Juniper Networks IDP Device (version IDP 50)

### Configuring to send Syslog Messages from SRX device

#### Using J-Web

1. Log in to the Juniper SRX device.
2. Click **Configure > CLI Tools > Point and Click CLI** in the Juniper SRX device.
3. Expand **System** and click **Syslog**.
4. In the **Syslog** page, click **Add New Entry** placed next to 'Host'.
5. Enter the IP address of the remote Syslog server (i.e., Firewall Analyzer).
6. Click **Apply** to save the configuration.

#### Using CLI

1. Log in to the Juniper SRX device CLI console.
2. Execute the following command:

```
user@host# set system syslog host <IP address of the remote Syslog server (i.e., Firewall Analyzer)> any any
```

The screenshot displays the ManageEngine Firewall Analyzer web interface. The top navigation bar includes 'Dashboard', 'Configure', 'Monitor', 'Maintain', and 'Troubleshoot'. The left sidebar shows a tree view of configuration options under 'Configuration', with 'syslog' selected. The main content area is titled 'System Syslog' and contains several sections:

- Buttons:** OK, Cancel, Refresh, Commit..., Discard...
- Archive:** A checkbox labeled 'Archive' is checked, with links for 'Edit' and 'Delete'.
- Source address:** A text input field with a help icon (?) to its right.
- Time format:** A checkbox labeled 'Time format' is unchecked, with a 'Yes' option.
- Console:** A section titled 'Console (None configured)' with a link 'Add new entry'.
- File:** A section titled 'File' with a link 'Add new entry' and a table listing log files.
- Host:** A section titled 'Host' with a link 'Add new entry' and a table listing log hosts.

| File name                            | Match | Nested Configuration | Actions                                     |
|--------------------------------------|-------|----------------------|---------------------------------------------|
| <a href="#">messages</a>             |       |                      | <a href="#">Edit</a> <a href="#">Delete</a> |
| <a href="#">interactive-commands</a> |       |                      | <a href="#">Edit</a> <a href="#">Delete</a> |

| Host name                      | Match | Facility override | Log prefix | Source address | Actions                                     |
|--------------------------------|-------|-------------------|------------|----------------|---------------------------------------------|
| <a href="#">192.168.170.20</a> |       |                   |            |                | <a href="#">Edit</a> <a href="#">Delete</a> |

To enable logging for Security policy:

#### Using J-Web

- Select **Configure > Security > Policy > FW Policies**.
- Click on the policy for which you would like to enable logging.
- Navigate to **Logging/Count** and in **Log Options**, select **Log at Session Close Time**.

#### Using CLI

1. Log in to the Juniper SRX device CLI console.
2. Execute the following command:

```
user@host# set security policies from-zone trust to-zone untrust policy permit-all then log session-close
```

**Edit Policy**

Policy | **Logging/Count** | Scheduling | Permit Action | Application Services

☒ **Enable Count**

Per Minute Alarm Threshold:  (0..4294967295 kbyte)

Per Second Alarm Threshold:  (0..4294967295 byte)

**Log Options**

Log at Session Close Time: ☒

Log at Session Init Time: ☐

### Juniper Networks IDP Device (version IDP 50)

Configuring to send Syslog Messages directly from Sensor

1. Log in to the Juniper Networks IDP device.
2. Click **Device > Report Settings > Enable Syslog** in the Juniper Networks IDP device.
3. Select the **Enable Syslog Messages** check box.
4. Click **Apply** to save the changes.

This configuration will generate syslogs for:

- All attacks
- Policy load
- Restart

This configuration will not provide:

- Profiler logs
- Device connect/disconnect logs
- Interface UP/DOWN logs
- Logs for Bypass State Changes

### Configuring to send Syslog Messages from NSM

1. Log in to NSM.
2. Click **Action Manager > Action Parameters > Define a Syslog Server** in the NSM.
3. Click **Action Manager > Device Log Action Criteria > Category** in the NSM.
4. Select **Category** = *all* and **Actions** = *syslog enable*
5. Click **Apply** to save the changes.

This configuration will generate syslogs for:

- All attacks
- Policy load
- Restart
- Profiler logs
- Device connect/disconnect logs

This configuration will not provide:

- Interface UP/DOWN logs
- Logs for Bypass State Changes

## Configuring 3Com

Firewall Analyzer supports the following 3Com Firewalls:

- 3Com X Family devices

### Obtaining Log Information

To create a Firewall Analyzer firewall profile, you must specify the log file location. 3Com firewalls do not create a log file. Instead, they direct a log stream to a syslog server which writes the log information to a file.

**Note:** The ManageEngine Firewall Analyzer Server(s) can be anywhere on the Network.

## X-Family Remote SysLog Configuration

To ensure that all the relevant syslog traffic is sent to the Firewall Analyzer, the X-family device needs configuration on several pages of the LSM. Enable remote syslog on the X-Family device, and configure it with the information required to communicate with the Firewall Analyzer Server(s).

1. Open a web browser browse to X-family device internal interface.
2. Login and navigate to **System > Configuration > Syslog Servers**.
3. Configure all four logs to be sent to the Firewall Analyzer.

**SYSTEM > CONFIGURATION > Syslog Servers**

To configure Syslog offload for Firewall rules you need to:

- Make sure you've checked the "Enable syslog logging" checkbox for the Firewall Rule you wish to log.
- Configure the Syslog Server in IPS > Action Sets > Notification Contacts > Remote Syslog. (These settings configure the Syslog server used to log Firewall Block rules.)
- Optionally, configure the Syslog Server here for "Firewall Session Log". (This setting configures the Syslog server used to log Firewall Permit and Web Filter rules.)

**Syslog Settings**

| Log Type             | Enable syslog offload                                                              | IP Address    |
|----------------------|------------------------------------------------------------------------------------|---------------|
| System Log           | <input checked="" type="checkbox"/> Enable syslog offload for System Log           | 192.368.1.208 |
| Audit Log            | <input checked="" type="checkbox"/> Enable syslog offload for Audit Log            | 192.368.1.208 |
| VPN Log              | <input checked="" type="checkbox"/> Enable syslog offload for VPN Log              | 192.368.1.208 |
| Firewall Session Log | <input checked="" type="checkbox"/> Enable syslog offload for Firewall Session Log | 192.368.1.208 |

**Apply**

4. Click **Apply**.
5. Navigate to **IPS > Action Sets > Notification Contacts > Remote System Log** and complete the form as shown below.



Additional syslog settings can be found on the [Syslog Servers](#) page.

### Remote Syslog Information

Log remotely to the following IP address(es):

IP Address:  Port:

Alert Facility:  Block Facility:

Delimiter:

Remote system log aggregation period:  minutes

[Add to table below](#)

| IP Address | Port | Alert Facility | Block Facility | Delimiter | Function(s) |
|------------|------|----------------|----------------|-----------|-------------|
|------------|------|----------------|----------------|-----------|-------------|

[Apply](#) [Cancel](#)

- Click **Add to table below**.

Additional syslog settings can be found on the [Syslog Servers](#) page.

### Remote Syslog Information

Log remotely to the following IP address(es):

IP Address:  Port:

Alert Facility:  Block Facility:

Delimiter:

Remote system log aggregation period:  minutes

[Add to table below](#)

**Changes will not be saved until you click "Apply"**

| IP Address    | Port | Alert Facility | Block Facility | Delimiter | Function(s) |
|---------------|------|----------------|----------------|-----------|-------------|
| 192.168.1.200 | 514  | 4              | 4              | tab       | ✗           |

[Apply](#) [Cancel](#)

- Click **Apply**.
- Navigate to **Firewall > Firewall Rules** and click **Create Firewall Rule**. Complete the form as shown below.

**Firewall Rule Setup (Basic)**

☒ **Enable Firewall Rule**

Action: **Permit**

Service: **Any**

Schedule: **Always**

Inactivity Timeout: **30** minutes

Comment:

☐ Enable local logging

☒ Enable syslog logging

☐ Skip IPS

☐ Enable Anti-Spam

☐ Enable Anti-Virus

☐ Enable Web-Filter

Web Profile: **Default**

**Network**

**Source**

Source Zone: **this-device**

Source IP:

- ☒ All IP Addresses
- ☐ IP Address Group: **NEO\_Phones**
- ☐ IP Subnet:  Mask:
- ☐ IP Range:  to

**Destination**

Destination Zone: **Any**

Destination IP:

- ☒ All IP Addresses
- ☐ IP Address Group: **NEO\_Phones**
- ☐ IP Subnet:  Mask:
- ☐ IP Range:  to

[Show Advanced Options](#)

**Create** **Cancel**

Note that later versions of TOS do not have separate checkboxes for **Enable local logging** and **Enable syslog logging** – they just have a checkbox for **Enable logging** which enables both.

9. Click **Create**. A new rule will be created at the bottom of the table.
10. Click **Create Firewall Rule**. Complete the form as shown below.

**Firewall Rule Setup (Basic)**

☒ **Enable Firewall Rule**

Action: **Block**

Service: **Any**

Schedule: **Always**

Inactivity Timeout: **30** minutes

Comment:

☐ Enable local logging

☒ Enable syslog logging

☐ Skip IPS

☐ Enable Anti-Spam

☐ Enable Anti-Virus

☐ Enable Web-Filter

Web Profile: **Default**

**Network**

**Source**

Source Zone: **Any**

Source IP:

- ☒ All IP Addresses
- ☐ IP Address Group: **NEO\_Phones**
- ☐ IP Subnet:  Mask:
- ☐ IP Range:  to

**Destination**

Destination Zone: **Any**

Destination IP:

- ☒ All IP Addresses
- ☐ IP Address Group: **NEO\_Phones**
- ☐ IP Subnet:  Mask:
- ☐ IP Range:  to

[Show Advanced Options](#)

**Create** **Cancel**

11. Click **Create**. A new rule will be created at the bottom of the table.

Please note that these last two rules must remain the last two rules in the Firewall Rule table. They replace two implicit "hidden" rules that are always present but do not support logging.



- Click the pencil icon next to the first rule in the Firewall Rule table. This will open the rule for edit, as in the example below.

The screenshot displays the 'Edit Firewall Rule' interface. On the left is a navigation menu with categories like IPS, Firewall, VPN, Events, System, Network, and Authentication. The main area is titled 'Firewall Rule Setup (Basic)'. It includes sections for enabling the rule, setting action and schedule, and defining network parameters. The 'Enable Firewall Rule' checkbox is checked. The 'Action' is set to 'Permit' and the 'Schedule' is 'Always'. In the 'Network' section, 'Source Zone' is 'LAN' and 'Destination Zone' is 'WAN'. Both 'Source IP' and 'Destination IP' are set to 'All IP Addresses'. The 'Enable syslog logging' checkbox is checked. At the bottom, there are 'Save' and 'Cancel' buttons.

- Click the **Enable syslog logging** checkbox as shown, then click **Save**.
- Repeat steps 12 and 13 for all the Firewall Rules until syslog logging is enabled on them all.

## Troubleshooting Operation with ManageEngine Analyzer

The Firewall Analyzer home page shows the “Dashboard” which is an overview of all the devices that are being monitored, showing traffic levels and security events that have been reported. The X-family device should appear here. If it does not, see the troubleshooting section below.

The following is a list of things to check if the ManageEngine Firewall Analyzer does not operate correctly:

- Check the syslog server settings on the X-family device are configured to point to the IP address of the Firewall Analyzer Server.
- Check that the Firewall Analyzer Server is listening on the same port (usually UDP 514) as the X-family syslog client is sending on.
- Check that any firewall device between the X-family and the Firewall Analyzer Server has a rule permitting traffic for UDP port 514.
- Check that there is no syslog daemon running on the same PC as the Firewall Analyzer Server – or it will take over port 514 which will stop the syslog data from going to the Firewall Analyzer Server.
- Traffic through the X-family device will only be counted if it is subject to a Firewall Rule and syslog logging is enabled for that rule. For example traffic will not be counted if:
  - it is passing between hosts in the same security zone
  - it is passing over a VPN or GRE tunnel to a host which is in the same zone as is used to terminate the VPN or GRE tunnel.

6. Events will not be generated for “hidden” firewall rules. At the time of writing, there are two implicit “hidden” firewall rules that are not displayed but act as if they were the last two rules in the Firewall Rule table. These are:  
Permit from this-device to ANY zone ANY protocol  
Block from ANY zone to ANY zone ANY protocol  
These rules do not generate log entries or syslog messages.  
To enable the Firewall Analyzer to monitor events that would be generated by these rules, two explicit rules must be created as the last two rules in the Firewall Rule table and syslog logging must be enabled on both of them.

## Configuring IPCop Firewalls

Firewall Analyzer supports IPCop Firewall Version 1.4.17 / 1.4.18

### Configuring IPCop To Send Audit Data To Firewall Analyzer

1. Open the **Log Settings Administrative Web Page**
2. **Log Settings:** This page allows you to control how the logs are displayed, specify the detail level and how long the log summaries are kept for, and control remote logging.
3. Click the **Save** button after making any changes to save the settings and restart the *syslogd* daemon.
4. **Sort in reverse chronological order:** Check the Sort in reverse chronological order checkbox if you want to see recent events at the top of a page, rather than at the bottom.
5. **Lines per page:** Select the number of log entries to display on a page from the Lines per page drop down menu. This can vary from between 15 and 500. Be aware that a large number of lines will take longer to process and display on slower hardware.
6. **Keep summaries for n days:** You can choose how long the logwatch summaries are kept on IPCop. If you are short of disk space, reduce the number of days.
7. **Detail level:** You can choose between *Low*, *Medium* and *High* levels of detail in the logwatch summaries from the **Detail level** drop down menu.
8. **Remote logging:** Select the **Enabled** checkbox to allow logging to a remote syslog server.
9. Specify the *hostname* or *hostname.domainname* or *IP Address* of the remote server in the Syslog server field provided. All logs will be forwarded to that server.
10. Remember to click the **Save** button after making any changes.

**Log Settings**

**Log viewing options**

Sort in reverse chronological order ☒ Lines per page: 50

---

**Log summaries**

Keep summaries for 56 days Detail level: High

---

**Remote logging**

Enabled: ☐ Syslog server:

Save

The IPCop will now send log data to Firewall Analyzer.

For more information, refer the IPCop documentation.

## Configure Proxy Server

### Configuring Proxy Servers

---

Firewall Analyzer listens at the default ports for exported log files. The following is a list of proxy servers and versions for which configuration instructions are included. Click the proxy server name to see the corresponding configuration instructions.

| Firewall Name                      | Version Numbers       |
|------------------------------------|-----------------------|
| <a href="#">Squid Proxy Server</a> | version 2.6 and above |

## Configuring Squid Proxy Server

For Squid v2.7 and above carry out the following configuration:

Carry out the following changes in the **services** file:

- Edit the **services** file in the */etc* directory
- Check the port in the syslog server settings UDP 514/1514 is UP
- Save the file and exit the editor

### Device Side Configuration

- Open the **squid.conf** file and find the below command:

*access\_log <location of file> squid*

Append the new command after the above command:

*access\_log udp://<Firewall Analyzer IP Address>:514/1514 squid*

- Restart the Squid Service

For Squid v2.6 carry out the following configuration:

### Device Side Configuration

- Open the **squid.conf** file and find the below command:

*access\_log <location of file> squid*

Append the new command after the above command:

*access\_log syslog squid*

- Restart the Squid Service

Carry out the following changes in the **syslog.conf** file:

- Login as root user and edit the **syslog.conf/rsyslog.conf** file in the */etc* directory
- Append *\*.\*<space/tab>@<server\_name>* at the end, where *<server\_name>* is the name of the machine on which Firewall Analyzer is running
- Save the configuration and exit the editor

Carry out the following changes in the **services** file:

- Edit the **services** file in the */etc* directory
- Check the port in the syslog server settings UDP 514/1514 is UP
- Save the file and exit the editor

Restart the syslog service on the host using the command:  
`/etc/rc.d/init.d/syslog restart`

### Configuring syslog-ng daemon in a Linux host

- Append the following entries at the end of **syslog-ng.conf** file in the `/etc/syslog-ng/` directory:

```
destination firewallanalyzer { udp("<server_name>" port(514)); };
log { source(src); destination(firewallanalyzer); };
```

where `<server_name>` is the IP address of the machine on which Firewall Analyzer is running.

- Restart syslog service

## Tips and Tricks

### Frequently Asked Questions

---

For the latest list of Frequently Asked Questions on Firewall Analyzer, visit the FAQ on the website or the public user forums.

#### General Product Information

1. Is a trial version of Firewall Analyzer available for evaluation?

Yes, a 30-day free trial version can be downloaded from the website at <http://www.fwanalyzer.com/>

2. Does the trial version have any restrictions?

The trial version is a fully functional version of Firewall Analyzer. When the trial period expires, you cannot restart the server.

3. Do I have to reinstall Firewall Analyzer when moving to the fully paid version?

No, you do not have to reinstall or shut down the server. You just need to enter the new license file in the Upgrade License box.

4. What other devices can Firewall Analyzer report on?

Apart from reporting on most enterprise firewall's, Firewall Analyzer can also analyze logs and generate specific reports on Squid Proxy servers.

5. I don't have a firewall, vpn, or a proxy server. Can I still use this product?

You can still use Firewall Analyzer to simulate firewall logs and see how reports will look like when real-time data is used. Click the **Simulate** link in the **Settings** tab to begin sending sample log files to Firewall Analyzer.

6. How many users can access the application simultaneously?

This depends only on the capacity of the server on which Firewall Analyzer is installed. The Firewall Analyzer license does not limit the number of users accessing the application at any time.

7. Firewall Analyzer runs in a web browser. Does that mean I can access it from anywhere?

Yes. As long as the web browser can access the server on which Firewall Analyzer is running, you can work with Firewall Analyzer from any location.

8. How secure is the data that is sent to the web browser over the Internet?

Data sent from Firewall Analyzer is normally not encrypted and hence is readable if intercepted.

9. How do I buy Firewall Analyzer?

You can buy Firewall Analyzer directly from the Zoho Corp. Online Store, or from a reseller near your location. Please see the website at <http://www.fwanalyzer.com/> for more information on purchasing options.

10. Is there a limit on the number of users or web sites that I can monitor?

There is no license restriction on the number of users or web sites that you can monitor. However, you may face performance issues when using lower end machines to run Firewall Analyzer.

## **Installation**

1. What are the recommended system requirements for Firewall Analyzer?

It is recommended that you install Firewall Analyzer on a machine with the following configuration:

- \* Processor - Pentium 4 - 1.5GHz
- \* Disk Space - 100MB \* RAM - 512MB
- \* Operating System - Windows 2000/XP, Linux 8.0/9.0
- \* Web Browser - Internet Explorer 6.0, or Mozilla Firefox 1.0

Look up System Requirements to see the minimum configuration required to install and run Firewall Analyzer.

2. Does the installation of Firewall Analyzer make any changes to the firewall server configuration?

The installation of Firewall Analyzer does not make any changes to the firewall server configuration.

3. Can I install Firewall Analyzer as a root user?

Firewall Analyzer can be started as a root user, but all file permissions will be changed, and later you cannot start the server as another user.

4. When I try to access the web client, another web server comes up. How is this possible?

The web server port you have selected during installation is possibly being used by another application. Configure that application to use another port, or change the Firewall Analyzer web server port.

5. Is a database backup necessary, or does Firewall Analyzer take care of this?

The archiving feature in Firewall Analyzer automatically stores all logs received in zipped flat files. You can configure archiving settings to suit the needs of your enterprise. Apart from that, if you need to backup the database, which contains processed data from firewall logs, you can run the database backup utility,



**BackupDB.bat/.sh** present in the <Firewall\_Analyzer\_Home>/troubleshooting directory.

6. How to configure Firewall Analyzer as service in Linux, after installation?

To configure Firewall Analyzer as service in Linux, after installation Normally, the Firewall Analyzer is installed as a service. If you have installed as an application and not as a service, you can configure it as a service any time later. The procedure to configure as service, start and stop the service is given below. To configure Firewall Analyzer as a service after installation, execute the following command. `sh configureAsService.sh -i` Usage of Firewall Analyzer service command `/bin # /etc/init.d/firewallanalyzer Usage: /etc/init.d/firewallanalyzer { console | start | stop | restart | status | dump }`

7. Can I use Java installation present in the Firewall Analyzer server machine? If yes, what is the procedure?

Yes, you can use Java installation present in the Firewall Analyzer server machine. The procedure is given below:

Copy and paste below files from Java bundled in the product to the Java existing in the machine for SMS functionality.

### Windows

- Copy `rxTxSerial.dll` file available in the <Firewall Analyzer Home>\jre\bin folder to `%JAVA_HOME%\jre\bin`
- Copy `RXTXcomm.jar` available in the <Firewall Analyzer Home>\jre\lib\ext to `%JAVA_HOME%\lib\ext`

**Note:** `%JAVA_HOME%` is the folder where JRE is installed on the server machine e.g., `C:\Program Files\Java\j2re1.4.1_01`

### Linux

- Copy `librxTxSerial.so` available in the <Firewall Analyzer Home>/jre/lib/i386 to `%JAVA_HOME%/jre/lib/i386`
- Copy `RXTXcomm.jar` available in the <Firewall Analyzer Home>/jre/lib/ext to `%JAVA_HOME%/jre/lib/ext`

**Note:** `%JAVA_HOME%` is the folder where JRE is installed on the server machine e.g., `/usr/local/j2sdk1.4.1_01` Copy `librxTxSerial.so` available in the <Firewall Analyzer

### Configuration

1. How do I see session information of all users registered to log in to Firewall Analyzer?

The session information for each user can be accessed from the **User Management** page. Click the **View** link under Login Details against each user to view the active session information and session history for that user. Look up User Management for more information on users in Firewall Analyzer.

2. How do I configure my firewall's to produce WELF log files?

Firewall's usually need to be configured specifically to generate log files in WELF. The Configuring Firewall's section includes configuration instructions for some of the firewall's supported by Firewall Analyzer.

3. My firewall cannot export logs. How do I configure Firewall Analyzer to report on my firewall?

You can set up Firewall Analyzer to import the logs from the firewall at periodic intervals.

4. Does Firewall Analyzer store raw logs?

Raw logs are archived periodically, and stored as zipped flat files. You can load these archived log files into Firewall Analyzer at any time and generate reports based on them.

5. How to assign Unassigned Protocols to Protocols and Protocol Groups?

### **Protocols in Reports**

Different firewalls denote the port numbers in the logs in different ways, for example, http:80 can be shown as tcp:80, http:80, etc. Hence, the protocol identifiers are grouped as **Protocols** and then to **Protocol Groups**. We found that the reports using Protocols are much usable than the reports based on port numbers. Hence, we show the Protocols in the reports. If all the unassigned protocols assigned to **Protocols** and **Protocol Groups**, there would not be any issue of unknown protocols.

### **Assigning Unassigned Protocols**

There will be some unassigned protocols as few protocols are not grouped.

You can view the port details of the unassigned protocols:

1. Click on the question mark icon beside the unassigned protocol group under **Traffic Statistics** in the home tab.
2. In the pop-up window, select **Last 6 hours**.
3. It will show all the unassigned protocols along with port numbers.

We have configured the generally used protocols as Groups like Mail, Web, FTP, Telnet, etc. However, you can group the unknown protocols as per your requirement. Configuring Unassigned Protocol will be a one-time activity.

1. Click on the **Unassigned** in **Protocol Group** under **Traffic Statistics**, which shows all the unknown protocols.
2. Click on **Assign** and Select **All** under Hits and select the **Multiple Selection**, which lists all the unassigned protocols.
3. Select the protocols and group it under **Protocol Group** and assign the appropriate protocol.
4. If you do not find a **Protocol Group**, click on the '+' sign to add a new **Protocol Group**.

**Note:** Once you assign the protocols, the reports will show the assigned protocols and the newly assigned protocols under their appropriate protocol group only from the assigned time. You will see the unassigned protocols in the reports generated earlier to the assigned time.

If you find that the reports based on ports, please assign specific protocols to the corresponding port numbers and create a custom report to view the details.

### Checking the port numbers

1. Check the port number by clicking on **Settings > Protocol Groups > Click** on the drop down menu against '**View by Group**' and select the appropriate protocol. This will show the protocol identifiers with port numbers.
2. You can also check the raw log in the folder *<Firewall Analyzer Home>\server\default\archive\<DNS(or)IP address\Hot>* folder to know the protocol type and port numbers (You can open the file using a notepad).

## Reporting

### General

1. Why am I seeing empty graphs?

Graphs are empty if no data is available. If you have started the server for the first time, wait for at least one minute for graphs to be populated.

2. What are the types of report formats that I can generate?

Reports can be generated in HTML, CSV, and PDF formats. All reports are generally viewed as HTML in the web browser, and then exported to CSV or PDF format. However, reports that are scheduled to run automatically, or be emailed automatically, are generated only as PDF files.

3. Are IP addresses automatically resolved?

IP addresses are automatically resolved by connecting to the network DNS server.

4. Why are some traffic values shown as 0.0 MB or 0.00%?

Since Firewall Analyzer processes log files as and when they are received, traffic values of 0.0MB or 0.0% may be displayed initially when the amount of traffic is less than 10KB. In such a case, wait until more data is received to populate the report tables.

5. What are the different formats in which reports can be exported?

Reports can be exported as PDF or CSV files. However, reports are emailed only as PDF files.

6. Why do the intranet reports show zero results?

Verify if intranet's have been configured correctly. If you have specified IP addresses that are not actually behind the firewall, you will get zero values in the reports.

## 7. Why don't trend reports take time values or top-n values into account?

Trend reports show historical data for the corresponding traffic statistics shown in the report. Hence time changes from the Global Calendar, or top-n value changes from the Show bar on the report, do not affect these reports.

## 8. Why the Un-used Rules Report is empty?

To view the "Un Used Rules Reports", you need to configure Firewall Analyzer to fetch rules from device via Telnet or SSH. After this configuration the reports will be available. However, this advanced feature is available only for Premium License Users of Firewall Analyzer.

## CheckPoint Firewall Reports

### 1. All the traffic reports are showing bytes value as zero?

Make sure you have set the Track value of your rules to **Account** in your CheckPoint management station. You can use Check Point Smart console to do the same. You can set the track value as *Account* for the rules that are allowing the traffic through your firewall's.

### 2. I am not getting VPN reports for CheckPoint firewall?

Firewall Analyzer looks for either the **vpn\_user** or **peer gateway** attributes in the logs received from your CheckPoint firewall's to generate VPN reports.

Example log is as follows:

```
id=leafirewall time="23Oct2006 9:49:30" action="encrypt" orig="testing"
i/f_dir="inbound" i/f_name="eth-s4p1 c0" has_accounting="1" product="VPN-1
& FireWall-1" __policy_id_tag="product=VPN-1 & FireWall-1[db_tag={C59340B0
-6276-11DB-B086-
00000000C2C2}];mgmt=testing;date=1161594819;policy_name=RKR_Policy]"
src="xxx.xxx.xxx.xxx" s_port="40555" dst="xxx.xxx.xxx.xxx" service="https"
proto="tcp" rule="15" scheme="IKE" dstkeyid="0x31b52e56" methods="ES P:
AES-256 + SHA1" peer gateway="mygateway" community="SECU"
start_time="23Oct2006 9:49:30" segment_time="23Oct 2006 9:49:30"
elapsed="0:00:09" packets="3" bytes="180" client_inbound_packets="3"
client_outbound_packets="0" server_inbound_packets="0"
server_outbound_packets="3" client_inbound_bytes="180"
client_outbound_bytes="0" server_inbound_bytes="0"
server_outbound_bytes="360" client_inbound_interface="eth-s4p1c0"
server_outbound_inter face="eth-s3p1c0" __pos="7" __nsons="0"
__p_dport="Unknown"
```

All the received logs are stored in *Firewall\_Analyzer\_Home\server\default\archive\* directory. You can browse through those logs to troubleshoot the problem.

If you find vpn related logs with other fields, then kindly send us the sample logs by uploading them to the following link:

<http://bonitas.zohocorp.com/upload/index.jsp?to=fwanalyzer-support@manageengine.com>

- I am not getting Attack Reports in CheckPoint firewall?

Firewall Analyzer looks for the attribute **attack** in the CheckPoint firewall logs to generate the attack reports.

- Firewall Analyzer shows the destination site (*example: www.yahoo.com*) but it is not showing the complete URL (*example: www.yahoo.com/index.html*)?

It looks for the attribute **resource** in the log.

Example log is as follows:

```
id=leafirewall time="16Aug2006 7:43:56" action="accept" orig="AHFW_1"
i/f_dir="outbound" i/f_name="eth0" has_accounting="1" product="VPN-1 &
FireWall-1" __policy_id_tag="product=VPN-1 & FireWall-1[db_tag={55E82635-
247B-44 B7-9E29-
42EDE0F57E2C};mgmt=FW_MGMT;date=1155671079;policy_name=N2H2_Filter
ed]" rule="22" rule_uid="{5A131CD7-BCBA -4859-AB39-43594A24931A}"
rule_name="HTTP Outbound" service_id="http" src="xxx.xxx.xxx.xxx"
s_port="2624" dst="xxx.xxx.xxx.xxx" service="http" proto="tcp"
xlatesrc="xxx.xxx.xxx.xxx" xlatesport="57700" xlatedport="Unknown" NAT
_rulenum="94" NAT_addtnl_rulenum="internal"
resource="http://www.yahoo.com/index.html" start_time="16Aug2006
7:43:56" segment_time="16Aug2006 7:43:56" elapsed="0:00:00" packets="11"
bytes="1161" client_inbound_packets="6" client_outbound_packets="5"
server_inbound_packets="5" server_outbound_packets="6"
client_inbound_bytes="753" client_outbound_bytes="408"
server_inbound_bytes="408" server_outbound_bytes="753"
client_inbound_interface="eth0" client_outbound_interface="eth0"
server_inbound_interface="eth1" server_outbound_interface="eth1" __pos="7"
__nsons="0"
```

- Why do I see zero results for kilobytes transferred in the reports for Check Point firewall?

This could be happening because bandwidth information is not being captured in the log file. Ensure that your Check Point firewall has been configured to generate both regular and accounting log files. While regular log files contain information regarding firewall activity, the accounting log file contains the bandwidth and session information. Please refer the Configuring Check Point Firewall's section for help on creating the accounting log file.

- I am getting only Unknown Events in Event Overview graphs in the dashboard?

CheckPoint firewall logs do not have the priority or severity fields. Event Overview graph groups Events based on severity. As there is no severity in check point logs, Firewall Analyzer puts default value as Unknown severity and hence Event Overview shows only Unknown Events. If you drill down that group or by clicking the More link, you can get complete Events.

## Cisco PIX Firewall Reports

1. I am not seeing Traffic reports in Cisco firewall's?
  1. In your Cisco PIX command line interface execute the command **show logging** and check the trap logging value.
  2. The trap logging should be set to informational for traffic logs to be generated from Cisco PIX firewall's. Execute the command **logging trap informational** to set the trap logging to informational.
  3. Ensure that no logs are disabled in Cisco PIX by executing the command **show logging disabled**
  4. Commonly, logs with id 302013,302014,302015 and 302016 are dealing with traffic. Make sure those ids are not disabled in your cisco firewall. If they are disabled then execute the command **logging message** to enable them.
2. I am not getting VPN reports for Cisco firewall's?

We can setup two kind of VPN's in Cisco firewall's as below.

### 1. Remote Host VPN:

This is between a User PC and the Cisco firewall's. User PC could be anywhere in the Internet. There are various technologies used to accomplish the same. Firewall Analyzer supports the following types.

#### o **IpSec:**

Firewall Analyzer supports IpSec remote host vpn in Cisco firewall's. Following are the sample logs generated:

#### **Cisco PIX:**

```
20_12_2005_09_00_20: <166>Dec 20 2005 09:52:14: %PIX-6-109005: Authentication succeeded for user 'john' from xxx.xxx.xxx.xxx/0 to xxx.xxx.xxx.xxx/0 on interface outside
```

```
20_12_2005_09_00_20: <166>Dec 20 2005 09:52:16: %PIX-6-602301: sa created, (sa) sa_dest= xxx.xxx.xxx.xxx, sa_prot= 50, sa_spi= 0x1e01c9b1(503433649), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 46
```

```
20_12_2005_09_00_20: <166>Dec 20 2005 09:52:16: %PIX-6-602301: sa created, (sa) sa_dest= xxx.xxx.xxx.xxx, sa_prot= 50, sa_spi= 0x94e99fdc(2498338780),V sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 45
```

```
20_12_2005_09_00_20: <166>Dec 20 2005 09:55:24: %PIX-6-602302: deleting SA, (sa) sa_dest= xxx.xxx.xxx.xxx, sa_prot= 50, sa_spi= 0x1e01c9b1(503433649), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 46
```

```
20_12_2005_09_00_20: <166>Dec 20 2005 09:55:24: %PIX-6-602302: deleting SA, (sa) sa_dest= xxx.xxx.xxx.xxx, sa_prot= 50,
```

*sa\_spi= 0x94e99fdc(2498338780), sa\_trans= esp-3des esp-md5-hmac , sa\_conn\_id= 45*

#### Cisco ASA:

*<166>:Apr 10 15:26:51 CDT: %PIX-vpn-6-602303: IPSEC: An inbound remote access SA (SPI= 0x2C4009CD) between xxx.xxx.xxx.xxx and xxx.xxx.xxx.xxx (user= ARNOLD) has been created*

*<166>:Apr 10 22:13:21 CDT: %PIX-vpn-6-602304: IPSEC: An inbound remote access SA (SPI= 0xA57F6150) between xxx.xxx.xxx.xxx and xxx.xxx.xxx.xxx (user= ARNOLD) has been deleted*

*<164>:Apr 10 20:13:23 CDT: %PIX-auth-4-113019: Group = TUMBUVPN, Username = ARNOLD, IP = xxx.xxx.xxx.xxx, Session disconnected. Session Type: IPSecOverUDP?, Duration: 4h:46m:39s, Bytes xmt: 1270639, Bytes rcv: 4292608, Reason: User Requested*

#### o PPTP:

Firewall Analyzer supports PPTP VPN between Cisco firewall and user's PC. Following are the sample logs generated:

*<133>Oct 20 2005 20:57:10: %PIX-6-603108: Built PPTP Tunnel at inside,tunnel-id = 25, remote-peer =xxx.xxx.xxx.xxx, virtual-interface = 1,client-dynamic-ip = xxx.xxx.xxx.xxx, username = king,MPPE-key-strength = number*

*<134>Oct 20 2005 20:58:01: %PIX-6-603109: Teardown PPPOE Tunnel at interface\_name, tunnel-id = 25,remote-peer = xxx.xxx.xxx.xxx*

*<134>Oct 20 2005 20:53:21: %PIX-6-603104: PPTP Tunnel created, tunnel\_id is 26, remote\_peer\_ip is xxx.xxx.xxx.xxx, ppp\_virtual\_interface\_id is 2,client\_dynamic\_ip is xxx.xxx.xxx.xxx, username is king, MPPE\_key\_strength is None*

*<134>Oct 20 2005 20:58:01: %PIX-6-603105: PPTP Tunnel deleted, tunnel\_id = 26, remote\_peer\_ip = xxx.xxx.xxx.xxx*

## 2. Site-To-Site VPN:

This vpn connection will be established between firewall to firewall. In most of the cases, this connection would have been established before the Firewall Analyzer installation. Also Cisco firewall's do no hint about the traffic that is going through this Site To Site VPN tunnel in the logs. In the Firewall Analyzer **VPN Reports**, there is no support for VPN connection types. However, in the **Traffic Reports**, you can filter the report using the IP Adresses assigned to the VPN connections to get the VPN traffic reports.



### 3. My Attack Reports displays "No Data Available"?

Cisco firewall's have inbuilt Intrusion Detection Systems (IDS) that detects the attacks. Firewall Analyzer supports all attack logs in Cisco firewall devices. All the attacks are identified by the cisco ids from 400000 to 400050. Apart from these logs, Firewall Analyzer also identifies supports ID's like 106016, 106017 etc. So if you find Attack reports empty there is a very valid chance that you have not received any attacks. To verify that you can go to `Firewall_Analyzer_Home\server\default\archive\` and search for the above ID's.

### 4. My Virus Reports are never getting populated?

In Cisco firewall's, all the doubtful activities will be identified as attacks and hence you will see all of them in Attack Reports. No Virus logs are given by Cisco Firewall's and hence there are no Virus Reports. You can very well remove the listing of Virus reports through report customization.

### 5. My Admin Reports displays "No Data Available"?

Firewall Analyzer reports login/logout attempts by searching the Cisco firewall logs for message ids like 611101, 611102, 611103, 605004, and 605005. Take a look at the logs available at `Firewall_Analyzer_Home\server\default\archive\` directory in case of any discrepancy.

### 6. What is the prerequisite for getting vdom/context Firewall reports for Cisco firewalls?

The Cisco Firewall IP address should be DNS resolvable from the Firewall Analyzer.

## NetScreen Firewall Reports (Syslog)

### 1. I am not getting any traffic reports. All SENT and RECEIVED values are shown as zero?

1. Make sure you have enabled traffic logs in your Netscreen.
2. In certain versions of NetScreen firewall there is an option to log the completed transaction whereas the other option is to log the initiated transaction. We recommend you to select the completed transaction option and deselect the initiated transaction option. This is because you can get the SENT and RECEIVED values only when the transaction is completed. You will find this check box while editing the rule.
3. Make sure you have enabled all logging levels upto informational. Because informational level logging includes traffic information

### 2. The VPN reports for my NetScreen firewall's are not getting populated?

Firewall Analyzer searches for **action=Tunnel** attributes in the NetScreen firewall logs to generate VPN reports.

### 3. I am not getting Virus reports for NetScreen firewall's?

Firewall Analyzer searches for the attribute **Virus** in the NetScreen firewall logs to generate Virus reports. Take a look at the log files available under `Firewall_Analyzer_Home/server/default/archive/` directory in case of any discrepancy.



## Other Firewall Reports (Sonicwall, Fortigate, and all other firewall's that support WELF)

### 1. My reports show *No Data Available*?

This means Firewall Analyzer has discovered your firewall and is able to recognize the logs. By default, as soon as you login, Firewall Analyzer shows data from current day's 00:00:00 hrs to current time of the machine where you are running Firewall Analyzer. There is a possibility that the firewall logs timestamp could be different from the Firewall Analyzer's timestamp. So just check *Firewall\_Analyzer\_Home/server/default/archive/* directory to view the firewall logs timestamp.

### 2. I am not getting any traffic reports?

Make sure you have enabled traffic logs and have set your logging level to informational. This is because most of the firewall's generate traffic logs only when logging level is set to informational.

### 3. The VPN reports for my firewall does not show any data?

Firewall Analyzer searches for attributes like **vpn=** or **vpnpolicy=** to generate VPN reports. So please verify whether your firewall logs have these attributes.

### 4. The Virus Reports for my firewall is not getting populated?

Firewall Analyzer searches for the attributes like **virus=** to generate the virus reports. Example logs are given below.

```
id=firewall time="2005-06-13 20:48:37" fw=FGT4002803033009 pri=5
src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_int=n/a dst_int=n/a service=http
status=passthrough from="n/a" to="n/a" file=trace.exe virus="Suspicious"
msg="The file trace.exe is infected with Suspicious. ref
http://www.fortinet.com/VirusEncyclopedia/search/encyclopediaSearch.do?metho
d=quickSearchDirectly&virusName=Suspicious.";
```

### 5. The Attack Reports for my firewall is not getting populated?

Firewall Analyzer searches for the attributes like **attack=** or **attack\_id=** to generate attack reports. Example logs are given below.

```
17_08_2005_16_54_03:id=firewall time="2005-08-18 00:59:03"
fw=FGT4002803033026 pri=1 attack_id=101974095 src=xxx.xxx.xxx.xxx
dst=xxx.xxx.xxx.xxx src_port=110 dst_port=58714 src_int=n/a dst_int=n/a
status=detected proto=6 service=58714/tcp msg="misc:
MS.Outlook.GMT.BufferOverflow,repeated 2 times[Reference:
http://www.fortinet.com/ids/ID101974095]";
```

### 6. I am not getting complete URLs for the destination sites?

Firewall Analyzer combines values of the fields like **dst/dstname** and **arg** to form the complete url. Kindly check whether your firewall generates the same in the log files available under *Firewall\_Analyzer\_Home/server/default/archive/* directory. Example logs are given below.

1902-01-16 08:52:47 Local0.Info 192.168.14.3 "id=firewall sn=0006B10C5210  
time="2006-01-06 15:53:30 UTC" fw=myfirwall pri=6 src=xxx.xxx.xxx.xxx  
dst=xxx.xxx.xxx.xxx proto=tcp/http op=GET sent=1533 rcvd=512 result=200  
**dstname=c.microsoft.com**  
**arg=/trans\_pixel.asp?source=msdn&TYPE=PV&p=library\_en-**  
**us\_cpguide\_html&URI=%2flibrary%2ft**

7. To display both Primary and Fail-over/Secondary Firewalls as single device in High Availability (Fail-over) mode of FortiGate Firewalls?

In order to get logs from primary and secondary Fortigate Firewall entities as one device, you have to set the **devName** field of failover or secondary firewall as **device\_id** field of primary firewall.

## Troubleshooting Tips

---

For the latest Troubleshooting Tips on Firewall Analyzer, visit the Troubleshooting Tips on the website or the public user forums.

### General [ Show/Hide All ]

1. Where do I find the log files to send to Firewall Analyzer Support?

The log files are located in the `<FirewallAnalyzer_Home>/server/default/log` directory. Typically when you run into a problem, you will be asked to send the **serverout.txt** file from this directory to Firewall Analyzer Support.

2. Internet Explorer says "Error opening this document. File cannot be found" when I try to open an exported PDF report.

Internet Explorer throws this error when you try to open an exported PDF report in the web browser itself. This is a known issue, and we are working on resolving it. For now, save the report to your local machine, and open it using the regular PDF software that you use (Adobe Acrobat Reader or xpdf)

3. I am having a Cisco PIX, but I only see Traffic IN and not Traffic OUT?
  - o You need to configure your Intranets in order to separate inbound and outbound traffic. The Inbound Outbound Traffic report will show the traffic details about inbound traffic ( traffic coming into LAN ) and outbound traffic ( traffic going out of LAN ) of the firewall. When configured, the Inbound Outbound Traffic Reports shows you which hosts and what protocol groups have been contributing the most traffic on either side of the firewall. Please follow the instructions available for Setting Up Intranets.
  - o Typical firewall logs are in the following format: `16.1.1.1 www.yahoo.com 10 bytes 1MB` (i.e. Source-IP Destination-IP Bytes-Sent Bytes-Received). But Cisco PIX does not provide a split-up of bytes-sent and bytes-received, but just provides a cumulative BYTES info. In most of the cases/protocols, RECEIVED will be more than SENT with respect to the source who originated the transaction. So we assume BYTES in Cisco PIX as RECEIVED. And in the case of FTP, Cisco PIX provides another log to identify the direction of the traffic. In that case, based on FTP put/get, we will determine whether the traffic is SENT or RECEIVED.

4. I find that Firewall Analyzer keeps crashing or all of a sudden stops collecting logs. What could be the reason?

The inbuilt MySQL database of Firewall Analyzer could get corrupted if other processes are accessing these directories. Kindly exclude the Firewall Analyzer installation directory 'ManageEngine' (it could be in `C:\ManageEngine` or `D:\ManageEngine`) from both the Backup process and Anti-Virus Scans.

5. How to increase the time limit of web client time out?

To increase the time limit of web client time out, follow the steps given below:

- Shutdown/stop the Firewall Analyzer application
- Rename/remove the C:\ME\Firewall\server\default\log directory into log\_old directory.
- Change the "session-timeout" value (default value is 30 minutes) as per your requirement (say 60 minutes), in the two files given below and save the files,
  - C:\ME\Firewall\server\default\conf\web.xml
  - C:\ME\Firewall\server\default\deploy\jbossweb-tomcat50.sar\conf\web.xml
- Restart the Firewall Analyzer Server.

The above changes will affect all the web clients connected to the FWA server.

Alternatively, you can install the "Auto IE Refresher" in your machine for IE browser and monitor the pages from your machine.

Reference pages:

<http://www.softpedia.com/get/Internet/Other-Internet-Related/Auto-IE-Refresher.shtml>  
[http://www.download.com/AutoRefresher-for-IE/3000-12512\\_4-10293579.html](http://www.download.com/AutoRefresher-for-IE/3000-12512_4-10293579.html)

## **Installation [ Show/Hide All ]**

1. Firewall Analyzer displays "Enter a proper ManageEngine license file" during installation.

This message could be shown in two cases:

**Case 1:** Your system date is set to a future or past date. In this case, uninstall Firewall Analyzer, reset the system date to the current date and time, and re-install Firewall Analyzer.

**Case 2:** You may have provided an incorrect or corrupted license file. Verify that you have applied the license file obtained from Zoho Corp.,

If neither is the reason, or you are still getting this error, contact [licensing@manageengine.com](mailto:licensing@manageengine.com)

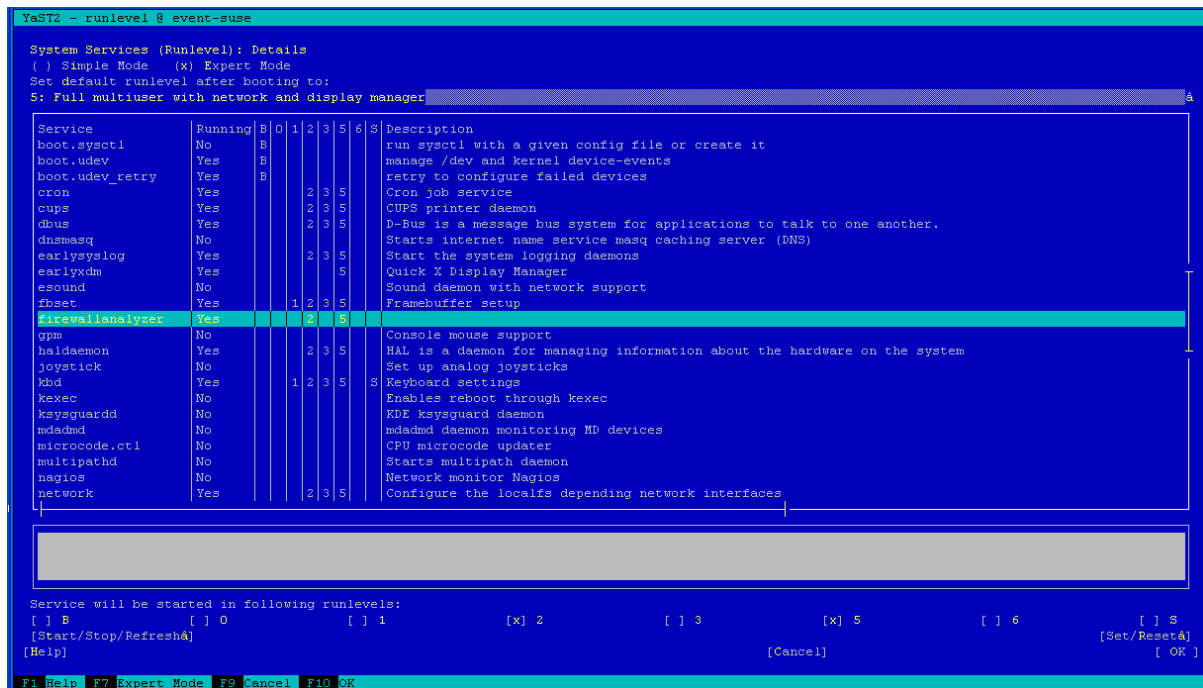
2. When I try to access the web client, another web server comes up. How is this possible?

The web server port you have selected during installation is possibly being used by another application. Configure that application to use another port, or change the Firewall Analyzer web server port.

3. Firewall Analyzer is running as a service in SUSE Linux machine. On reboot, Firewall Analyzer service is not getting started. How to overcome this?

If Firewall Analyzer is running as a service in SUSE Linux machine and on reboot the Firewall Analyzer service is not getting started, carry out the following procedure.

- Open a Command window with Super User privileges, on the SUSE Linux machine
- Execute the YaST program. The **YaST Control Center** screen opens up
- In that, select **System > System Services (Runlevel)** menu. The **System Services (Runlevel): Details** screen open up.
- In the table displayed, select the Expert Mode and *firewallanalyzer* service.
- Set the default runlevel after booting to 2 & 5. Refer the image given below.
- Select **Set** and **OK**
- Exit the command window
- Now reboot the machine again



## Startup and Shut Down [ Show/Hide All ]

1. MySQL-related errors on Windows machines.

**Probable cause:** An instance of MySQL is already running on this machine

**Solution:** Shut down all instances of MySQL and then start the Firewall Analyzer server.

**Probable cause:** Port 33336 is not free

**Solution:** Kill the other application running on port 33336. If you cannot free this port, then change the MySQL port used in Firewall Analyzer.

2. Firewall Analyzer displays "Port 8500 needed by Firewall Analyzer is being used by another application. Please free the port and restart Firewall Analyzer" when trying to start the server.

**Probable cause:** The default web server port used by Firewall Analyzer is not free.

**Solution:** Kill the other application running on port 8500. If you cannot free this port, then change the web server port used in Firewall Analyzer.

3. Unable to start the application in Linux

**Probable cause:** It is due to invalid host information in the *etc/hosts* directory.

**Solution:** Change it to the following format, you will be able to start the application and get reports.

`/etc/hosts`

Entry should be like:

`127.0.0.1 mini localhost`

## Importing Logs

1. Firewall Analyzer not importing logs from mapped network drive, if Firewall Analyzer is running as service.

**Solution:** Instead of giving mapped network drive, you give UNC path (`\\ComputerName\SharedFolder\Resource`) (e.g., `\\cherry\log\isa_log*.w3c`).

If the issue still persist, check the following:

- The account in which Firewall Analyzer service runs must have full privilege to that shared drive
- If the Firewall Analyzer machine is in a domain `xxxxx` and the shared machine/drive is in a workgroup (i.e., cross domain), Firewall Analyzer will not fetch the logs unless the full domain admin privilege is available.

## Reporting

1. Why am I seeing empty graphs?

**Probable cause:** Graphs are empty either because there is no traffic is passing through the firewall or if firewall traffic is not sufficient enough to populate the reports table of Firewall Analyzer.

**Solution:** If you are starting Firewall Analyzer for the first time or if you are shutting down and restarting Firewall Analyzer, it will wait for the reports table to be populated with 5000 log records for the first time. From the next time onwards, Firewall Analyzer will populate reports table once in 7 minutes or once it receives the next 5000 records, whichever is earlier. You can check for the number of records received in " Packet Count " icon shown in top right corner in client UI. This will list out the details like the number of logs received and also the

last received log time. It is better to run the server continuously and check whether 5000 records are collected. Do not stop and restart the server in-between!

Moreover, for viewing the already collected log records in the reports, kindly do the following:

1. Login into Firewall Analyzer client UI. You will be seeing the Dashboard page.
2. Replace the URL shown in your browser with the following URL.

*<http://localhost:8500/fw/genreport.do>*

3. Wait for sometime. Once the reports are generated an empty page will be shown.
4. Now remove *genreport.do* from the URL and just type *<http://localhost:8500/fw>* alone.
5. Now you will be able to see the report data.

2. I can't see the Live Reports for my SonicWALL firewall

You cannot see Live Reports for SonicWALL firewalls because the time duration attribute is not supported in the SonicWALL log files.

3. Why are some traffic values shown as 0.0MB or 0.0%?

Since Firewall Analyzer processes log files as and when they are received, traffic values of 0.0MB or 0.0% may be displayed initially when the amount of traffic is less than 10KB. In such a case, wait until more data is received to populate the report tables.

4. Why do I see zero results for kilobytes transferred in the reports for Check Point firewall?

This could be happening because bandwidth information is not being captured in the log file. Ensure that your Check Point firewall has been configured to generate both regular and accounting log files. While regular log files contain information regarding firewall activity, the accounting log file contains the bandwidth and session information.

5. Why do the Intranet Reports show zero results?

Verify if intranets have been configured correctly. If you have specified IP addresses that are not actually behind the firewall, you will get zero values in the reports.

6. Why doesn't Trend Reports take time values or top-n values into account?

Trend reports show historical data for the corresponding traffic statistics shown in the report. Hence time changes from the Global Calendar, or top-n value changes from the **Show** bar on the report, do not affect these reports.

7. My firewall is sending WELF logs, but the reports do not show any URL information?

Firewall Analyzer checks for the entry "**arg=your URL**" in the firewall logs to populate and show URL in report data. If this entry is not present in the firewall logs then the reports wouldn't be showing any URL information.

8. In the Compliance Report field, the following message appears: *'Unable to generate compliance report. Reason: Failed to locate Nipper. Click here to enable it'*. What should I do?

#### Supported Platform:

- Ubuntu 9.1.10
- Fedora 12
- OpenSuSE 11.2
- CentOS 5.5

#### Prerequisite:

The GNU/Linux platform requires Qt 4.5 to be installed. Your package manager system should automatically install this for you.

#### Steps:

1. Download Nipper libraries from <http://www.manageengine.com/products/firewall/download-third-party-utilities.html> according to your platform
2. Install the rpm or deb according to your Operating System
3. Connect to Firewall Analyzer web client and type the following URL:  
*'http://<host name>:8500/fw/userConfig.do'*
4. In that, there is an option to provide the path in which you have installed 'Nipper'. For ex: *'/usr/bin/nipper'*
5. Click on **Save** link

After performing the above steps, go to **Setting > Device Rule > Add Device Info**, the option to generate compliance report for the device will be enabled.



## Other Tools and Utilities

### Configuring Firewall Analyzer Parameters

You can configure Firewall Analyzer to handle .

#### Firewall Analyzer User Input Configuration

To carry out the advanced configuration in the Firewall Analyzer, access the following URL in the browser:

*http://<hostname of Firewall Analyzer>:8500/fw/userConfig.do*

The **Firewall Analyzer User Input Configuration** page will be displayed.

Enter the values and select the options as per your requirement.

| Configuration Parameters    |                                                            |              |
|-----------------------------|------------------------------------------------------------|--------------|
| Data Crunching Limit Value  |                                                            | Save   Reset |
| PDF Report Row Count        | 10                                                         | Save   Reset |
| Minimum Disk Space Setting  | 5                                                          | Save   Reset |
| Destination By Port         | true/false                                                 | Save         |
| Nipper Location             | <The location where Nipper is installed, only for Linux>   | Save         |
| Context Based Config Change | true/false                                                 | Save         |
| Admin User Groups           | <User groups that have admin access to Juniper SSLVPN box> | Save   Reset |
| Virtual Firewalls           | Select your Firewall Name, <names of Firewalls>            | Save         |

The parameters which can be configured are explained below:

- **Data Crunching Limit Value:**

It allows you to set the number of rows to be moved from one level to another level say for example hourly to daily, daily to monthly etc.

- **PDF Report Row Count:**

It allows you to choose the number of rows that you want to see in the PDF report. Allowable range is 10 to 100.

- **Minimum Disk Space Setting:**

It allows you to set the minimum disc space (in GB) at which you would like to get warned.

- **Destination By Port:**

Applicable for Cisco PIX device. Setting this parameter allows Firewall Analyzer to decide the destination based on the minimum value between source and destination ports.

- **Nipper Location:**

For linux installation, provide the location where Nipper is installed. (ex: /use/bin/nipper )

**Admin User Groups:**

For Juniper SSLVPN box, provide the user groups that have admin access (Each group should be comma separated. For Eg: Admin Users,Employee\_Administrator).

**Context Based Config Change:**

By setting this parameter,Firewall Analyzer will provide context based email notification for firewall configuration changes.

- **Virtual Firewalls:**

Unselect the device to disable virtual firewall detection.Select the checkbox to enable it.

## Configuring MSSQL Database

Firewall Analyzer lets users to configure and use MSSQL database.

The procedure to configure the MSSQL is applicable **only for fresh installation of Firewall Analyzer** server.

If you are already using the Firewall Analyzer with MySQL and you want to change the database to MSSQL, please refer the **Migrating Firewall Analyzer Data from MySQL to MSSQL Database** page and follow the procedure given there.

The steps to configure and run the Firewall Analyzer server with SQLSERVER as the database is given below:

1. From the installed MS SQLSERVER, copy the files **bcp.exe** and **bcp.rll** to *<Firewall Analyzer Home>\mysql\bin* folder.

**Note:** If you are copying the above file from SQL Server (Version 2005 & above) installed server and the Firewall Analyzer is installed in other machine, please install the following SQL Native Client in the Firewall Analyzer machine as per the SQL version and CPU type of Firewall Analyzer machine.

### MSSQL 2005 (32 bit)

<http://download.microsoft.com/download/4/4/d/44dbde61-b385-4fc2-a67d-48053b8f9fad/sqlncli.msi>



### MSSQL 2005 (64 bit)

[http://download.microsoft.com/download/4/4/d/44dbde61-b385-4fc2-a67d-48053b8f9fad/sqlncli\\_x64.msi](http://download.microsoft.com/download/4/4/d/44dbde61-b385-4fc2-a67d-48053b8f9fad/sqlncli_x64.msi)

### MSSQL 2008 (32 bit)

<http://go.microsoft.com/fwlink/?LinkId=123717&clcid=0x409>

### MSSQL 2008 (64 bit)

<http://go.microsoft.com/fwlink/?LinkId=123718&clcid=0x409>

2. Invoke the *<Firewall Analyzer Home>\tools\changeDBServer.bat*, to configure the MS SQLSERVER credentials like ServerName, Port, UserName and Password.

3. **Database Setup Wizard** pops-up.
4. In the wizard screen, select **Server Type** as *SQL Server*. **Available SQL Server Instances** are listed in a combo box. Enter the **Host Name** and **Port** of the SQL Server from the instances.
5. Select the authentication type using the "**Connect Using:**" options.
6. The options are:
  - a. Windows Authentication

For Windows Authentication, enter the **Domain Name**, **User Name** and **Password**. Ensure that both Firewall Analyzer server and SQL Server are in the same domain and logged in with the same Domain Administrator account.

**Database Setup Wizard**

Server Type: **SQL Server**

Host Name: **FELOG-W2K8**

Port: **1433**

Available SQL Server Instances

- FELOG-W2K8;MSSQLSERVER;1433
- FELOG-W2K8;SQLEXPRESS;49410
- FELOG-W2K8;MSSQLSERVER;1433
- FELOG-W2K8;MSSQLSERVER;1433

☒ **Windows Authentication** ☐ **SQL Server Authentication**

Domain Name: **felog-w2k8**

User Name: **administrator**

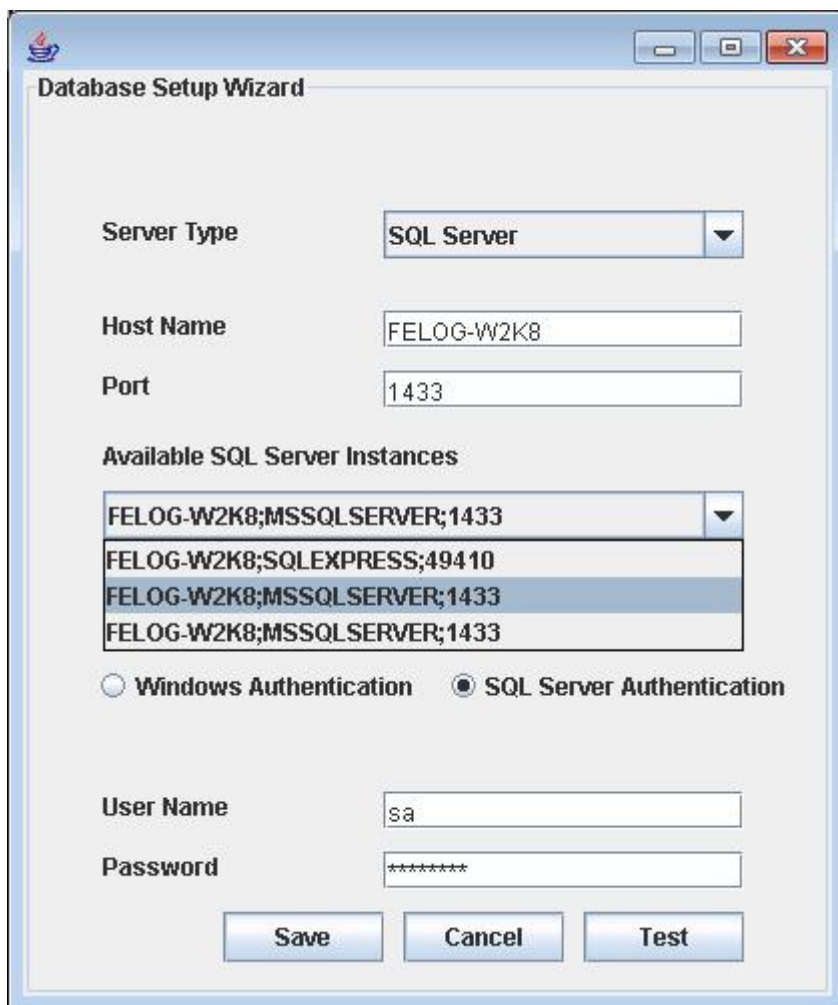
Password: **\*\*\*\*\***

**Save** **Cancel** **Test**

- b. SQL Server Authentication

For SQL Server Authentication, enter the **User Name** and **Password**.

While configuring the database with SQL Server Cluster installation, need to select the desired instance listed under the Available SQL Server Instances as shown in the below:



**Database Setup Wizard**

Server Type: **SQL Server**

Host Name: **FELOG-W2K8**

Port: **1433**

Available SQL Server Instances:

- FELOG-W2K8;MSSQLSERVER;1433
- FELOG-W2K8;SQLEXPRESS;49410
- FELOG-W2K8;MSSQLSERVER;1433
- FELOG-W2K8;MSSQLSERVER;1433

☐ Windows Authentication ☒ SQL Server Authentication

User Name: **sa**

Password: **\*\*\*\*\***

**Save** **Cancel** **Test**

7. Click **Test** button to check whether the credentials are correct. If the test fails, the credentials may be wrong, recheck and enter the correct credentials.
8. If you are not able to get the SQL Server instances, please check the following in the SQL Server:
  - o SQL server is not installed in the selected machine.
  - o There is a firewall blocking port **1434** on the server
  - o If you are using **SQL Server 2005**, please start the '**SQL Server Browser**' from the Services.



9. Click **Save** button to save the SQL Server configuration. Note that, it will take few minutes to configure the settings of the SQL Server database.
10. Start the Firewall Analyzer Server/Service to work with the MS SQLSERVER as the database.

From the installed MS SQLSERVER, copy the files **bcp.exe** and **bcp.rll** to *<Firewall Analyzer Home>\mysql\bin* folder.

## Moving Firewall Analyzer's database to different directory in the same server

To move the Firewall Analyzer's Indexes to a different drive/directory on the same server

- Go to **Archive Settings** page.
- Enable **Change Raw Logs Indexing Location** check box.
- Modify the Log Indexing Location to the new location and save.
- Move all the directories from previous location to the new location.

### How to move MySQL data to another drive in the same physical machine?

Follow the steps given below to move the database to a different drive:

- Stop the Firewall Analyzer server/service, if it is running.
- Check the task manager for the process **java.exe** and **mysqld-nt.exe**, kill the process if any of these process is running.
- Copy the folder *<Firewall Analyzer Home>\mysql\data* to a folder in another drive (e.g., *D:\Firewall\data*).i.e., the new location to which you want to move the data of MySQL database.
- Rename the present **data** folder under **mysql** folder as **dataold** and you can delete it later.
- Open the **startDB.bat/sh** file, located under *<Firewall Analyzer Home>\bin* directory.

#### For Windows:

Edit the following command in the mysql startup line:

```
--datadir=%DB_HOME%\data
as
--datadir=D:\Firewall\data
```

where, the *D:\Firewall\data* is the new location for the MySQL database.

After changing the command, the **start** command will look like:


```
@start /B %DB_HOME%\bin\mysqld-nt --standalone --
basedir=%DB_HOME%
--port=%DB_PORT% --datadir=D:\Firewall\data --
innodb_buffer_pool_size=180M
--key-buffer-size=32M --innodb_file_per_table --max_heap_table_size=32M
--tmp_table_size=40M --innodb_flush_log_at_trx_commit=0 --log-error
```

#### For Linux:

Please add "**--datadir=<desired location>**" after "**--basedir**" attribute in the mysql startup line.

After adding the "--datadir" attribute to the command, the **start** command will look like:

```
#default
$DB_HOME/bin/mysqld --no-defaults --basedir=$DB_HOME --
datadir=/advent/5g/Working/Latest/data --port=$DB_PORT --
socket=$TMP_HOME/mysql.sock --user=root.....
```

|                                                                                   |                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>The above command may slightly differ for various builds, however, ensure that,<br/> in Windows "--datadir=%DB_HOME%\data"<br/> is changed to "--datadir=&lt;new drive with absolute path&gt;"<br/> <b>or</b><br/> in Linux "--datadir=&lt;new drive with absolute path&gt;" is added.</p> |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- Save the file.
- Start the Firewall Analyzer server/service.
- Check whether the data is correct and the *D:\Firewall\data* directory size is getting increased.

### Moving MSSQL Database

1. Stop the Firewall Analyzer Server/Service.
2. Login to SQL Server database with system administrator permissions.
3. Find the current location of the data file and log file for the database firewall by using the following commands:

```
use firewall
go
sp_helpfile
go
```

4. Detach the database by using the following commands:

```
use master
go
sp_detach_db 'firewall'
go
```

5. Copy the data file and log file from the current location (<MSSQL Home>\data\firewall.mdf and <MSSQL Home>\data\firewall\_log.LDF) to the new location (<New location>\firewall.mdf and <New Location>\firewall\_log.LDF).
6. Re-attach the database and point to the new location by using the following commands:

```
use master
go
sp_attach_db 'firewall' , '<New Location>\firewall.mdf' , '<New Location>\firewall_log.LDF'
go
```



7. Verify the changed location by using the following commands:

```
use firewall
```

```
go
```

```
sp_helpfile
```


```
go
```

Start the Firewall Analyzer Server/Service.

## Moving Firewall Analyzer Server installation to another server


- Moving Firewall Analyzer installation to new server with MySQL
- Moving Firewall Analyzer installation to new server with MS SQL
- Moving Archive, Index files to new server

### How to move Firewall Analyzer installation to a new server?

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p><b>Ensure that the License file in the old server is copied to the new server after moving the Firewall Analyzer to the new server.</b></p> <p>Before moving the Firewall Analyzer installation to a new machine, ensure that the build of the old installation is latest. If not, upgrade in the old installation to the latest build and proceed further. To find out the build number:</p> <ul style="list-style-type: none"> <li>• You can click on <b>About</b> link in the top right hand corner, the build number will be displayed in the About pop-up screen.</li> <li>• If you are not able to open the UI, go to the folder C:\ManageEngine\Firewall\troubleshooting and open the file <b>build.properties</b> in a notepad, you can find the build number in the file.</li> </ul> |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Follow the steps given below to move Firewall Analyzer installation to a different server:

1. Stop the Firewall Analyzer server/service.
2. Check the Windows Task Manager for the processes '**java.exe**' and '**mysqld-nt.exe**', if any of these processes is running, kill only the Firewall Analyzer related process.
3. Copy the following folders (including the files and sub-folders) completely to another drive or to a mapped network drive as a precautionary measure. This will help us to restore the settings and data in-case of any issue with the new machine.
  - a. The folder, '**MySQL**' located under *<Firewall Analyzer Home>\.*
  - b. The folder, '**Archive**' located under *<Firewall Analyzer Home>\server\default\archive\.*
4. Download and install the latest build of Firewall Analyzer from the following link in the new server:  
<http://manageengine.com/products/firewall/download.html>
5. **Once you install the application in the new machine, ensure that you do not start the application or shutdown the application, if started.**
6. Rename the folder *<Firewall Analyzer Home>\MySQL* as '**MySQLori**'.
7. Copy the MySQL folder (which is located under *<Firewall Analyzer Home>\MySQL*) from the old machine to the new machine in the same location.

|                                                                                     |                                                                                                                                          |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p><b>Take extra care and ensure that the Firewall Analyzer is not running on both the machines while performing this operation.</b></p> |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|

8. Restart the Firewall Analyzer on the new machine and check whether the data and configurations are intact.

#### **To move the Firewall Analyzer's Indexes to new server**

- Go to **Archive Settings** page.
- Enable **Change Raw Logs Indexing Location** check box.
- Modify the Log Indexing Location to the new location and save.
- Move all the directories from previous location to the new location.

#### **Procedure to move Firewall Analyzer Server installation to another server for MSSQL database**

1. Stop Firewall Analyzer server/service.
2. Download and install the latest build of Firewall Analyzer from the following link:  
<http://manageengine.com/products/firewall/download.html>
3. Once you install the application in the new machine, kindly make sure that you do not start the application or shutdown the Firewall Analyzer if started.
4. Please configure the MSSQL server credentials of the earlier Firewall Analyzer server installation as explained in the **Configuring MSSQL Database** topic.
5. Start the Firewall Analyzer server/service on the new machine and check whether the data and the configurations are intact.

## Running Firewall Analyzer and MySQL database in different machines

### How to run Firewall Analyzer server and MySQL server in different machines?

Carry out following steps to run the MySQL server in a separate machine.

- Stop the Firewall Analyzer server/service.
- Edit `<Firewall Analyzer Home>/server/default/deploy/mysql-ds.xml` with the following line.  
  
`<connection-url>jdbc:mysql://localhost:33336/firewall</connection-url>`
- Instead of localhost, enter the IP address/hostname of the machine in which you intend to run MySQL server.
- Edit `<Firewall Analyzer Home>/server/default/conf/nms-service.xml` file and change **StartDBServer** value to *false*. By default its value will be *true*.
- Carry out the following steps in MySQL server machine
  - Install Firewall Analyzer if it is not installed or if you do not have MySQL server installed here.
  - Edit `<Firewall Analyzer Home>/bin/startDB.bat/sh` to tune MySQL parameters as given in the following sizing guide.  
[http://manageengine.com/products/firewall/system\\_requirement.htm](http://manageengine.com/products/firewall/system_requirement.htm)
  - Execute `<Firewall Analyzer Home>/bin/startDB.bat/sh` to start MySQL server. Ensure that you never start the application in this machine.
- Start the Firewall Analyzer in the Firewall Analyzer machine. You should be able to see the reports



Start the MySQL server first in the MySQL server machine and then start the Firewall Analyzer application in the Firewall Analyzer server machine.

## Configuring Secure Communication - SSL

The SSL protocol provides several features that enable secure transmission of Web traffic. These features include data encryption, server authentication, and message integrity.

You can enable secure communication from web clients to the Firewall Analyzer server using SSL.



The steps provided describe how to enable SSL functionality and generate certificates only. Depending on your network configuration and security needs, you may need to consult outside documentation. For advanced configuration concerns, please refer to the SSL resources at <http://www.apache.org> and <http://www.modssl.org>

- **Generating a valid certificate**
- **Disabling HTTP**
- **Enabling HTTPS (SSL)**
- **Verifying SSL Setup**
- **Configuring HTTPS Configuration Parameters for 64 bit/128 bit encryption**
- **Using the existing SSL certificate**
- **How to install SSL certificate for Firewall Analyzer**

### Generating a valid certificate

Stop the server, if it is running.

Follow the instructions given below for SSL Installation:

If you have a keystore file for using HTTPS, place the file under *<Firewall Analyzer Home>\server\default\conf* directory and rename it as "**chap8.keystore**"

### Disabling HTTP

When you have enabled SSL, HTTP will continue to be enabled on the web server port (default 8080). To disable HTTP follow the steps below:

1. Edit the **server.xml** file present in *<Firewall Analyzer Home>/server/default/deploy/jbossweb-tomcat50.sar* directory.
2. Comment out the HTTP connection parameters, by placing the `<!--` tag before, and the `-->` tag after the following lines:

```
<Connector port="8080" address="{jboss.bind.address}"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>
```

## Enabling HTTPS (SSL)

- In the same file, enable the HTTPS connection parameters, by removing the <!-- tag before, and the --> tag after the following lines:

```
<!--
<Connector port="8443" address="{jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="{jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```



While creating keystore file, you can enter the password as per your requirement. But ensure that the same password is configured, in the **server.xml** file. Example password is configured as '**rmi+ssl**'.

## Verifying SSL Setup

1. Restart the Firewall Analyzer server.
2. Verify that the following message appears in the command window after the Firewall Analyzer application is started:

```
Server started.
Please connect your client at https://localhost:8500
```

3. Connect to the server from a web browser by typing `https://<hostname>:8500` where `<hostname>` is the machine where the server is running

## Configuring HTTPS Configuration Parameters for 64 bit/128 bit encryption

If you want to configure the HTTPS connection parameters for 64 bit/128 bit encryption, add the following parameter at the end of the SSL/TLS Connector tag:

```
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"
```

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="{jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="{jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

## Using the existing SSL certificate

- You can export the Wild card certificate to a **.pfx** file and then follow the instructions given below to configure the same in Firewall Analyzer.
- Stop ManageEngine Firewall Analyzer service
- Copy the **.pfx** file to the location *<Firewall Analyzer Home>\server\default\conf*
- Go to the location *<Firewall Analyzer Home>\server\default\deploy\jbossweb-tomcat50.sar* and open the file **server.xml** in word pad, and locate the entries in the file as below:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="{jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="{jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

- Replace the file name *chap8.keystore* with the pfx file name (**<pfx file name>.pfx**) and also enter the **keystoreType="pkcs12"** after the file name and also replace the **keystorePass** value 'rmi+ssl' with the password for the **.pfx** file.
- The entries should be as given below:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="{jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="{jboss.server.home.dir}/conf/<pfx file name>.pfx"
keystoreType="pkcs12"
keystorePass="<password for the .pfx file>" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

- Restart Firewall Analyzer service.

## How to install SSL certificate for Firewall Analyzer

Follow the instructions given below for SSL Installation:

### Step 1: Create a new Keystore

1. You will be using the keytool command to create and manage your new Keystore file. When you are ready to create your keystore go to the directory where you plan to manage your Keystore and certificates (*<Firewall Analyzer Home>\jre\bin\*). Enter the following command:

```
keytool -genkey -alias <our_alias_name> or [Domain Name] -keyalg
RSA -keystore chap8.keystore
```

(For example: **keytool -genkey -alias tomcat -keyalg RSA -keystore chap8.keystore**)

2. You will be prompted to choose a password for your keystore. You will then be prompted to enter your Organization information. When it asks for first and last name, DO NOT mention your first and last name, but rather it is your Fully Qualified Domain Name for the site you are securing say, helpdesk.yourdomain.com. If you are ordering a Wildcard Certificate this must begin with the \* character say, \*.yourdomain.com)
3. After you have completed the required information confirm that the information is correct by entering 'y' or 'yes' when prompted. Next, you will be asked for your password to confirm. Make sure to remember the password you choose. Your keystore file named **chap8.keystore** is now created in your current working directory.

### Step 2: Generate a CSR from your new keystore

1. Next, you will use keytool to create the Certificate Signing Request (CSR) from your Keystore. Enter the following command

**keytool -certreq -alias <your\_alias\_name> or [Domain Name] -file csr.txt -keystore chap8.keystore**  
(For example: **keytool -certreq -alias tomcat -file csr.txt -keystore chap8.keystore**)

2. Type the keystore password that you chose earlier and hit Enter.
3. Your CSR file named **csr.txt** is now created in your current directory. Open the CSR with a text editor, and copy and paste the text (including the BEGIN and END tags) into the CA web order form. Be careful to save the keystore file (chap8.keystore) as your certificates will be installed to it later.

### Step 3: How to install your SSL Certificate

1. Download your Certificate files from the email from CA to the directory where your keystore (chap8.keystore) was saved during the CSR creation process. The certificate must be installed to this exact keystore. If you try to install it to a different keystore it will not work. The certificates you downloaded must be installed to your keystore in the correct order for your certificate to be trusted. If the certificates are not installed in the correct order, then the certificate will not authenticate properly.
2. Install the Root Certificate file:
  - o Each time you install a certificate to your keystore you will be prompted for the keystore password, which you chose when generating your CSR.
  - o Type the following command to install the Root certificate file:

**keytool -import -trustcacerts -alias root -file TrustedRoot.crt -keystore chap8.keystore**

**NOTE:** Choose 'Yes' if you get prompted with a message that says "Certificate already exists in system-wide CA keystore under alias <entrustsslca> Do you still want to add it to your own keystore? [no]:" You will get a confirmation stating that the "Certificate was added to keystore".



3. Install the intermediate certificates if any. (Follow the instructions provided by the CA)
4. Install the Primary Certificate file:
  - o Type the following command to install the Primary certificate file:

```
keytool -import -trustcacerts -alias tomcat -file
<your_domain_name>.crt -keystore chap8.keystore
```

This time you should get a slightly different confirmation stating that the "Certificate reply was installed in keystore" If it asks if you want to trust the certificate. Choose y or yes. Your Certificates are now installed to your keystore file (keystore.key) and you just need to configure your server to use the keystore file.


## How to bind specific interface of the machine to Firewall Analyzer application?

### How to bind specific interface of the machine to Firewall Analyzer application?

- For customers of **version 6.0** or higher
- For customers of **version 5.0** or lesser

#### For customers of version 6.0 or higher

- For Windows Machine: (running as application)
- For Windows Machine: (running as service)
- For Linux Machine: (running as application)
- For Linux Machine: (running as service)

|                                                                                     |                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• In Windows, for commenting batch files add "rem" before the command and for uncommenting remove the "rem" before the command.</li> <li>• In Linux, for commenting sh files add "#" before the command and for uncommenting remove the "#" before the command.</li> </ul> |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### For Windows Machine: (running as application and not as service)

- Shutdown Firewall Analyzer.
- Open the **startDB.bat** file which is under *<Firewall Analyzer Home>\bin* directory and go to "**MYSQL Start Command Block**", follow the instructions over there, make necessary changes and save the file.
- Open the **stopDB.bat** file which is under *<Firewall Analyzer Home>\bin* directory and go to "**command Arguments settings block**", follow the instructions over there, make necessary changes and save the file.
- Open the **run.bat** file which is under *<Firewall Analyzer Home>\bin* directory and go to "**RESTART Command block**", follow the instructions over there, make necessary changes and save the file.
- Open **setcommonenv.bat** file which is under *<Firewall Analyzer Home>\bin* directory and go to "**JAVA\_OPTS Setting command Block**", follow the instructions over there, make necessary changes and save the file.
- Open the **mysql-ds.xml** file which is under *<Firewall Analyzer Home>\server\default\deploy* directory and **replace localhost in connection-url tag with the <ip-address>** to which you wants to bind the application and save the file.
- Open the **sample-bindings.xml** file which is under *<Firewall Analyzer Home>\server\default\conf* directory and go to "**jboss port setting block**", follow the instructions over there, make necessary changes and save the file.
- Restart Firewall Analyzer.



To shutdown Firewall Analyzer use the below command  
`shutdown.bat -S -s <ip-address>: <jndi-port>`  
 where **<jndi-port>** in the above command is the one which you have set in **sample-bindings.xml**

#### For Windows machine (running as service)

- Stop the Firewall Analyzer service.
- Open the **startDB.bat** file which is under *<Firewall Analyzer Home>\bin* directory and go to "**MYSQL Start Command Block**", follow the instructions over there, make necessary changes and save the file.
- Open the **stopDB.bat** file which is under *<Firewall Analyzer Home>\bin* directory and go to "**command Arguments settings block**", follow the instructions over there, make necessary changes and save the file.
- Open the **wrapper.conf** file which is under *<Firewall Analyzer Home>\server\default\conf* and go to "**Adding Application Parameters Block**", follow the instructions over there, make necessary changes and save the file.
- Open the **mysql-ds.xml** file which is under *<Firewall Analyzer Home>\server\default\deploy* directory and **replace localhost in connection-url tag with the <ip-address>** to which you wants to bind the application and save the file.
- Start the Firewall Analyzer service.

#### For Linux Machine: (running as application and not as service)

- Shutdown Firewall Analyzer.
- Open the **startDB.sh** file which is under *<Firewall Analyzer Home>/bin* directory and go to "**MYSQL Start Command Block**", follow the instructions over there, make necessary changes and save the file.
- Open the **stopDB.sh** file which is under *<Firewall Analyzer Home>/bin* directory and go to "**command Arguments settings block**", follow the instructions over there, make necessary changes and save the file.
- Open the **run.sh** file which is under *<Firewall Analyzer Home>/bin* directory and replace the existing jboss main arguments "`-LAdventNetDeploymentSystem.jar`" with these arguments "`-LAdventNetDeploymentSystem.jar" "-c default" "-b <ip-address>`" and replace **<ip-address>** with the ip-address to which you wants to bind your application and save the file.

Before changing, the jboss main arguments will be  
`org.jboss.Main "-LAdventNetDeploymentSystem.jar"`

After changing the arguments, it will be  
`org.jboss.Main "-LAdventNetDeploymentSystem.jar" "-c default" "-b <ip-address>"`

- Open **setcommonenv.sh** file which is under *<Firewall Analyzer Home>/bin* directory and go to "**JAVA\_OPTS Setting command Block**", follow the instructions over there, make necessary changes and save the file.

- Open the **mysql-ds.xml** file which is under *<Firewall Analyzer Home>/server/default/deploy* directory and **replace localhost in connection-url tag with the <ip-address>** to which you wants to bind the application and save the file.
- Open the **sample-bindings.xml** file which is under *<Firewall Analyzer Home>/server/default/conf* directory and go to "**jboss port setting block**", follow the instructions over there, make necessary changes and save the file.
- Restart Firewall Analyzer.

To shutdown Firewall Analyzer use the below command

```
./shutdown.sh -S -s <ip-address>:<jndi-port>
```

where **<jndi-port>** in the above command is the one which you have set in **sample-bindings.xml**

Ensure that the following two conditions are met:

1. In **.etc/nsswitch.conf** file you need to ensure the below line:

*hosts: files dns*

i.e. it should be in the order 'files' and 'dns' not the reverse as 'dns' and 'files'.

i.e. it should not be *hosts: dns files*

2. In **.etc/hosts** file add the below one as the first line

*<binded-ip-address> localhost*

Replace **<binded-ip-address>** with the ip-address to which you want to bind your application.

#### For Linux Machine: (running as service)

- Stop the Firewall Analyzer service.
- Open the **startDB.sh** file which is under *<Firewall Analyzer Home>/bin* directory and go to "**MYSQL Start Command Block**", follow the instructions over there, make necessary changes and save the file.
- Open the **stopDB.sh** file which is under *<Firewall Analyzer Home>/bin* directory and go to "**command Arguments settings block**", follow the instructions over there, make necessary changes and save the file.
- Open the **wrapper.conf** file which is under *<Firewall Analyzer Home>/server/default/conf* and go to "**Adding Application Parameters Block**", follow the instructions over there, make necessary changes and save the file.
- Open the **mysql-ds.xml** file which is under *<Firewall Analyzer Home>/server/default/deploy* directory and **replace localhost in connection-url tag with the <ip-address>** to which you wants to bind the application and save the file.
- Start the Firewall Analyzer service.

## For customers of version 5.0 or lesser

- For Windows Machine: (running as application)
- For Windows Machine: (running as service)
- For Linux Machine: (running as application)
- For Linux Machine: (running as service)



Through out the below document, replace **<ip-address>** with the IP address with which you wants to bind the application.

## For Windows Machine: (running as application and not as service)

- Shutdown Firewall Analyzer.
- Open the **startDB.bat** file which is under *<Firewall Analyzer Home>\bin* directory and add option **--bind-address=<ip-address>** in the **mysqld start** command that starts with *@start* and save the file.
- Open the **stopDB.bat** file which is under *<Firewall Analyzer Home>\bin* directory and add **-h <ip-address>** to the command arguments and save the file.

After the change the line should like the one given below:

```
set commandArgs=-P %PORT% -u %USER_NAME% -h <ip-address>
```

- Open the **run.bat** file which is under *<Firewall Analyzer Home>\bin* directory and add the arguments **-c default -b <ip-address>** to the *jboss.Main* as given below:

```
:RESTART
"%JAVA%" %JAVA_OPTS% -classpath "%JBOSS_CLASSPATH%"
org.jboss.Main %ARGS% -c default -b <ip-address> %*
```

and save the file.

- Open **setcommonenv.bat** file which is under *<Firewall Analyzer Home>\bin* directory and add the option **-Dspecific.bind.address=<ip-address>** while setting *JAVA\_OPTS* as given below:

```
set JAVA_OPTS=-Djava.library.path=..\lib;..\lib\native -DpdfReport=false -
Duser.country=US -Duser.language=en -DminDiskSpace=5 -Xms128m -
Xmx512m -Dspecific.bind.address=<ip-address>
```

and save the file.

- Open the **mysql-ds.xml** file which is under *<Firewall Analyzer Home>\server\default\deploy* directory and **replace localhost in connection-url tag with the <ip-address>** to which you wants to bind the application and save the file.
- Open the **sample-bindings.xml** file which is under *<Firewall Analyzer Home>\server\default\conf* directory and go to "**jboss port setting block**", set any fixed **RMI port/jndi port** (provided the port should be free) and save the file.

Before setting the port it will look like `<binding host="{jboss.bind.address}" port="0"/>`

After setting the port it will look like `<binding host="{jboss.bind.address}" port="<any fixed free port>"/>`

**<any fixed free port>** is the port number which you have configured and not used by any application.

- Restart Firewall Analyzer.



To shutdown Firewall Analyzer use the below command

`shutdown.bat -S -s <ip-address>: <jndi-port>`

where **<jndi-port>** in the above command is the one which you have set in **sample-bindings.xml**

### For Windows machine (running as service)

- Stop the Firewall Analyzer service.
- Open the **startDB.bat** file which is under `<Firewall Analyzer Home>\bin` directory and add option **--bind-address=<ip-address>** in the **mysqld start** command that starts with `@start` and save the file.
- Open the **stopDB.bat** file which is under `<Firewall Analyzer Home>\bin` directory and add **-h <ip-address>** to the command arguments and save the file.

After the change the line should like the one given below:

`set commandArgs=-P %PORT% -u %USER_NAME% -h <ip-address>`

- Open the **wrapper.conf** file which is under `<Firewall Analyzer Home>\server\default\conf` and follow the below steps:  
Uncomment the second application parameter  
**"wrapper.app.parameter.2=-L../lib/AdventNetDeploymentSystem.jar"**.  
Add the following new application parameters

**wrapper.app.parameter.3=-c default**

**wrapper.app.parameter.4=-b <ip-address>**

**wrapper.app.parameter.5=-Dspecific.bind.address=<ip-address>**

and save the file.



Remove **"#"** symbol for uncommenting in the **.conf** file.

- Open the **mysql-ds.xml** file which is under `<Firewall Analyzer Home>\server\default\deploy` directory and **replace localhost in connection-url tag with the <ip-address>** to which you wants to bind the application and save the file.
- Start the Firewall Analyzer service.

## For Linux Machine: (running as application and not as service)

- Shutdown Firewall Analyzer.
- Open the **startDB.sh** file which is under *<Firewall Analyzer Home>/bin* directory and add option **--bind-address=<ip-address>** in the **mysqld start** command that starts with *\$DB\_HOME* and save the file.
- Open the **stopDB.sh** file which is under *<Firewall Analyzer Home>/bin* directory and add **-h <ip-address>** to the command arguments and save the file.

Before change the line will look like the one given below:

```
commandArgs="-S $TMP_HOME -P $DB_PORT -u $USER_NAME"
```

After the change the line should like the one given below:

```
commandArgs="-S $TMP_HOME -P $DB_PORT -u $USER_NAME -h <ip-address>"
```

- Open the **run.sh** file which is under *<Firewall Analyzer Home>/bin* directory and replace the existing jboss main arguments **"-LAdventNetDeploymentSystem.jar"** with these arguments **"-LAdventNetDeploymentSystem.jar" "-c default" "-b <ip-address>"** and replace **<ip-address>** with the ip-address to which you wants to bind your application and save the file.

Before changing, the jboss main arguments will be  
*org.jboss.Main "-LAdventNetDeploymentSystem.jar"*

After changing the arguments, it will be  
*org.jboss.Main "-LAdventNetDeploymentSystem.jar" "-c default" "-b <ip-address>"*

- Open **setcommonenv.sh** file which is under *<Firewall Analyzer Home>/bin* directory and add the option **-Dspecific.bind.address=<ip-address>** while setting *JAVA\_OPTS* as given below:

```
JAVA_OPTS="-Djava.awt.headless=true -DpdfReport=false -
Duser.language=en -Duser.country=US -DminDiskSpace=5 -
Djava.library.path=../lib:../lib/native -Xms128m -Xmx512m -
Dspecific.bind.address=<ip-address>"
```

and save the file.

- Open the **mysql-ds.xml** file which is under *<Firewall Analyzer Home>/server/default/deploy* directory and **replace localhost in connection-url tag with the <ip-address>** to which you wants to bind the application and save the file.
- Open the **sample-bindings.xml** file which is under *<Firewall Analyzer Home>/server/default/conf* directory and go to **"jboss port setting block"**, set any fixed **RMI port/jndi port** (provided the port should be free) and save the file.



Before setting the port it will look like `<binding host="{jboss.bind.address}" port="0"/>`

After setting the port it will look like `<binding host="{jboss.bind.address}" port="<any fixed free port>"/>`

**<any fixed free port>** is the port number which you have configured and not used by any application.

- Restart Firewall Analyzer.

To shutdown Firewall Analyzer use the below command

```
./shutdown.sh -S -s <ip-address>: <jndi-port>
```

where **<jndi-port>** in the above command is the one which you have set in **sample-bindings.xml**

Ensure that the following two conditions are met:

1. In **.etc/nsswitch.conf** file you need to ensure the below line:

```
hosts: files dns
```

i.e. it should be in the order 'files' and 'dns' not the reverse as 'dns' and 'files'.

i.e. it should not be `hosts: dns files`

2. In **.etc/hosts** file add the below one as the first line

```
<binded-ip-address> localhost
```

Replace **<binded-ip-address>** with the ip-address to which you want to bind your application.

#### For Linux Machine: (running as service)

- Stop the Firewall Analyzer service.
- Open the **startDB.sh** file which is under `<Firewall Analyzer Home>/bin` directory and add option **--bind-address=<ip-address>** in the **mysqld start** command that starts with `$DB_HOME` and save the file.
- Open the **stopDB.sh** file which is under `<Firewall Analyzer Home>/bin` directory and add **-h <ip-address>** to the command arguments and save the file.

Before change the line will look like the one given below:

```
commandArgs="-S $TMP_HOME -P $DB_PORT -u $USER_NAME"
```

After the change the line should like the one given below:

```
commandArgs="-S $TMP_HOME -P $DB_PORT -u $USER_NAME -h <ip-address>"
```

- Open the **wrapper.conf** file which is under `<Firewall Analyzer Home>\server\default\conf` and follow the below steps:  
Uncomment the second application parameter



```
"wrapper.app.parameter.2=-
L../lib/AdventNetDeploymentSystem.jar".
```

Add the following new application parameters

```
wrapper.app.parameter.3=-c default
wrapper.app.parameter.4=-b <ip-address>
wrapper.app.parameter.5=-Dspecific.bind.address=<ip-
address>
and save the file.
```



Remove "#" symbol for uncommenting in the **.conf** file.

- Open the **mysql-ds.xml** file which is under *<Firewall Analyzer Home>/server/default/deploy* directory and **replace localhost in connection-url tag with the <ip-address>** to which you wants to bind the application and save the file.
- Start the Firewall Analyzer service.

## How to move Firewall Analyzer Raw Logs Archive and Raw Logs Indexing directory to mapped network drive?

To move the Firewall Analyzer Raw Logs Archive and Raw Logs Indexing directory to mapped network drive, the procedure is slightly different for running the Firewall Analyzer as an application and service.

The procedure to move to mapped network drive is given separately.

- Firewall Analyzer started as application
- Firewall Analyzer started as service

### Firewall Analyzer started as application

In the remote machine in which you want to store raw logs archive and indexing, carry out the following procedure:

- Create/select the folder in the remote machine.
- Ensure that the remote machine is available in the same network.
- Share the selected/created folder.

In the Firewall Analyzer server machine, carry out the following procedure:

- Open Windows Explorer.
- Select **Tools > Map Network Drive...** menu.
- The **Map Network Drive** window pops-up.
- Select the drive name in the **Drive** drop down menu, as per your requirement.
- Select the shared folder of the remote machine in the **Folder** text box. Use the **Browse** button to select the shared.
- Click **Finish** button. The pop-up window closes.

After carrying out the above steps, carry out the procedure in the Firewall Analyzer client for "**How to move Firewall Analyzer Raw Logs Archive and Raw Logs Indexing directory?**"

- Click the **Settings** tabs on the top of the client.
- Click on **Archived Files**. *Archived Files* page opens up.
- Click **Archive Settings**. *File Archive Settings* page pops-up.
  - Select **Change Raw Logs Archive Location** option and change the path of the Raw Logs Archive location. Ensure that you give the mapped networked drive path, where you want to move the archive files storage. For example: **Z:\Firewall\archive**  
The default path is <Firewall Analyzer Home>server\default\archive
  - Select the option **Change Raw Logs Indexing Location** and change the path of the Raw Logs Index files storage location. The default path is <Firewall Analyzer Home>\server\default\indexes

**Note:** After you configure the new location for the Raw Log Index files, ensure that you copy all the files and sub-folders of the **hot**, **warm**, and **cold** sub-folders of the **indexes** folder from the existing location to the newly configured location.

### Firewall Analyzer started as service

**In the remote machine in which you want to store raw logs archive and indexing, carry out the following procedure:**

- Create/select the folder in the remote machine.
- Ensure that the remote machine is available in the same network.
- Share the selected/created folder.
- Configure the access credentials of a specific user account of the Firewall Analyzer server machine, to the shared folder.

In the Firewall Analyzer server machine, carry out the following procedure:

- Ensure that you logon to the Firewall Analyzer server machine with the same credentials of the user account. The user account credentials to which the folder in the remote machine is shared for access.
- Select the **Start > Control Panel** menu.
- In the *Control Panel*, select the **Administrative Tools > Services**.
- Select the **ManageEngine Firewall Analyzer** service.
- Stop the service.
- Right click the service and select the **Properties** menu.
- In the **ManageEngine Firewall Analyzer Properties** pop-up window, select **Log On** tab.
- In the Log On tab, select **Log on as: This Account:**.
- Enter the credentials of the user account. The user account credentials to which the folder in the remote machine is shared for access.
- Change to **General** tab.
- Click **Start** button to start the **Manage Engine Firewall Analyzer** service.
- Click **OK** to close the **ManageEngine Firewall Analyzer Properties** window.

After carrying out the above steps, carry out the procedure in the Firewall Analyzer client for "**How to move Firewall Analyzer Raw Logs Archive and Raw Logs Indexing directory?**"

- Click the **Settings** tabs on the top of the client.
- Click on **Archived Files**. *Archived Files* page opens up.
- Click **Archive Settings**. *File Archive Settings* page pops-up.
  - Select **Change Raw Logs Archive Location** option and change the path of the Raw Logs Archive location. Ensure that you enter the absolute path of the mapped network drive, where you want to move the archive files storage. For example: **\\<Shared Machine>\<Shared Folder>**  
The default path is *<Firewall Analyzer Home>server\default\archive*
  - Select the option **Change Raw Logs Indexing Location** and change the path of the Raw Logs Index files storage location.  
The default path is *<Firewall Analyzer Home>\server\default\indexes*

**Note:** After you configure the new location for the Raw Log Index files, ensure that you copy all the files and sub-folders of the **hot**, **warm**, and **cold** sub-folders of the **indexes** folder from the existing location to the newly configured location.

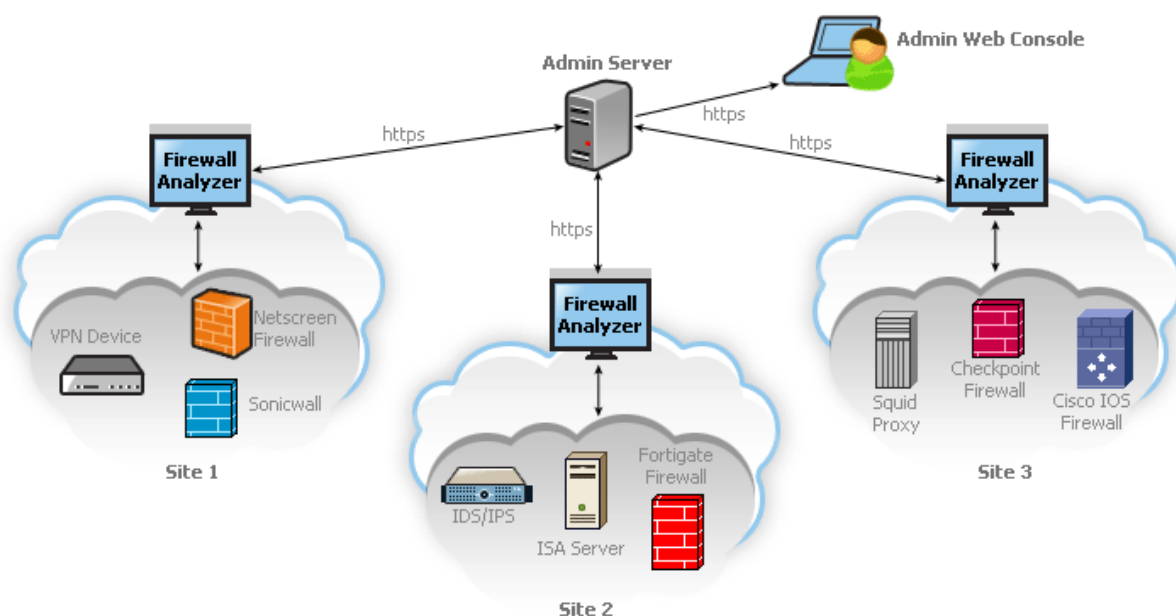
## Distributed Edition - Collector Server

### Introduction - Firewall Analyzer Distributed Edition Collector Server

An enterprise spread across geography finds it difficult to manage the Firewalls in different branch office locations. To simplify this task Firewall Analyzer provides Distributed Edition. This edition employs distributed model.

### What is Firewall Analyzer Distributed Edition?

**Firewall Analyzer Distributed Edition** is a distributed setup of Firewall Analyzers. It consists of one Admin server and N number of Collector servers. The Collector servers are installed at different geographical locations (one per LAN environment) and connected to the Admin server. This allows the network administrators to access the details of the Firewalls at different remote locations in a central place. All the reports, alerts and other Firewall information can be accessed through one single console. The administrator of large enterprises with various branch locations through out the globe stand benefited with this edition. For Managed Security Service Providers (MSSP) it is a boon. They can monitor the Collector server installed at different customer places from one point.



**Firewall Analyzer Distributed Edition addresses requirements like the following:**

- Aggregated Firewall log management of whole enterprise in different physical locations.
- Scalable architecture supporting 100s of Firewalls.
- Centralized monitoring using single console view.
- Secured communication using HTTPS.
- Exclusive segmented and secured view for various customers of MSSP.

This User Guide will help you install Firewall Analyzer distributed set up, and get familiar with the Firewall Analyzer Admin server user interface. If you are unable to find the information you are looking for in this document, please let us know at [fwanalyzer-support@manageengine.com](mailto:fwanalyzer-support@manageengine.com)

## Installing and Uninstalling - Distributed Edition Collector Server

Firewall Analyzer is available for Windows and Linux platforms. For more information on supported versions and other specifications, look up System Requirements.

This topic covers the following procedures:

- Installing Firewall Analyzer
  - Windows
  - Linux
- Uninstalling Firewall Analyzer
  - Windows
  - Linux

### Installing Firewall Analyzer

#### Windows:

The Firewall Analyzer Windows download is available as an EXE file at:

<http://manageengine.com/products/firewall/download.html>


Double-click the downloaded EXE file, and follow the instructions as they appear on screen.



1. Ensure that the Distributed Edition - Admin Server, you intend to connect this Collector Server, is running.
2. Ensure that you configure the Admin Server details correctly during the Collector Server installation procedure. Otherwise, the Collector Server installation will be incomplete. The Admin Server details are validated only at the end of the installation procedure.

- Click **Advanced Install** button.
- Read the *License Agreement* and click **Yes** button.
- Select **Distributed Edition** and click **Next** button.
- Select **Collector** and click **Next** button.
- In Collector Configuration, enter **Admin Server Host**, retain or modify **Admin Server Port**, select **Use HTTPS** if Admin Server is using secure communication (**https**) or else un-select this option. If the Collector Server is behind Proxy Server, select **Use a Proxy Server to contact Admin Server** check box. Configure the **Proxy Server Host**, **Proxy Server Port**, **User Name**, and **Password** details. Click **Next** button.
- Select **Destination Folder** using **Browse** button, for installation. Click **Next** button.
- Retain or modify the Web Port of Collector Server and select the Language of Installation from the combo box. Three languages are supported for installation and they are Chinese, English, and Japanese. By default English is selected. Click **Next** button.
- Select **Install Firewall Analyzer as service** check box (recommended), if you want to install Collector server as a service. Click **Next** button.

- Configure new Program Folder or retain the default. Click **Next** button.
- The installation details like Installation Directory, Program Folder, and Web Port are displayed. Click **Next** button.
- Now, Distributed Edition - Collector server installation is complete.

Once the installation is complete you will notice a  tray icon, which provides you with the following options.

| Option                        | Description                                                                                                                                                  |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Firewall Server Status</b> | This option provides you details like <i>Server Name</i> , <i>Server IpAddress</i> , <i>Server Port</i> , <i>Server Status</i> .                             |
| <b>Start WebClient</b>        | This option will open up your default browser and connect you to the web login UI of Firewall Analyzer Server, provided the server has already been started. |
| <b>Shutdown Server</b>        | This option will shutdown the Firewall Analyzer Server.                                                                                                      |



The tray icon option is only available for Windows !

### Linux:

The Firewall Analyzer Linux download is available as a BIN file at <http://manageengine.com/products/firewall/download.html>

1. Download the BIN file, and assign **execute** permission using the command:  
`chmod a+x <file_name>.bin`  
 where *<file\_name>* is the name of the downloaded BIN file.
2. Execute the following command: `./<file_name>.bin`



During installation if you get an error message stating that the temp folder does not have enough space, try executing this command with the `-is:tempdir <directory_name>` option, where *<directory\_name>* is the absolute path of an existing directory. `./<file_name>.bin -is:tempdir <directory_name>`

3. Follow the instructions as they appear on the screen.



1. Ensure that the Distributed Edition - Admin Server, you intend to connect this Collector Server, is running.
2. Ensure that you configure the Admin Server details correctly during the Collector Server installation procedure. Otherwise, the Collector Server installation will be incomplete.

- Click **Advanced Install** button.
- Read the *License Agreement* and click **Yes** button.
- Select **Distributed Edition** and click **Next** button.
- Select **Collector** and click **Next** button.
- In Collector Configuration, enter **Admin Server Host**, retain or modify **Admin Server Port**, select or unselect **HTTPS** check box as per requirement. If the

Collector Server is behind Proxy Server, select **Use a Proxy Server to contact Admin Server** check box. Configure the **Proxy Server Host**, **Proxy Server Port**, **User Name**, and **Password** details. Click **Next** button.

- Select **Destination Folder** using **Browse** button, for installation. Click **Next** button.
- Retain or modify the Web Port of Collector Server and select the Language of Installation from the combo box. Three languages are supported for installation and they are Chinese, English, and Japanese. By default English is selected. Click **Next** button.
- Select **Install Firewall Analyzer as service** check box (recommended), if you want to install Collector server as a service. Click **Next** button.
- Configure new Program Folder or retain the default. Click **Next** button.
- The installation details like Installation Directory, Program Folder, and Web Port are displayed. Click **Next** button.
- Now, Distributed Edition - Collector Server installation is complete.

This will install Firewall Analyzer - Collector server on the respective machine.

## Uninstalling Firewall Analyzer

### Windows:

1. Navigate to the Program folder in which Firewall Analyzer has been installed. By default, this is **Start > Programs > ManageEngine Firewall Analyzer 6**.
2. Select the option **Uninstall Firewall Analyzer**.
3. You will be asked to confirm your choice, after which Firewall Analyzer is uninstalled.

### Linux:

1. Navigate to the *<Firewall Analyzer Home>/server/\_uninst* directory.
2. Execute the command `./uninstaller.bin`
3. You will be asked to confirm your choice, after which Firewall Analyzer is uninstalled.



At the end of uninstallation you will be taken to the Uninstallation Feedback Form where you can provide reasons for your product uninstallation. This would help us improve this product.

## **Troubleshooting Tips - Distributed Edition Collector Server**

---

For the latest Troubleshooting Tips on Firewall Analyzer, visit the Troubleshooting Tips on the website or the public user forums.



# Integrating Firewall Analyzer with OpManager

You can integrate Firewall Analyzer with OpManager.

## Pre-requisites

To integrate Firewall Analyzer with OpManager

- OpManager application should be installed and running.
- Firewall Analyzer application should be installed and running.
- The Servers and Firewalls, whose logs you want to monitor and analyze must be discovered/added in OpManager and Firewall Analyzer.
- The Firewall Analyzer settings must be configured properly in OpManager.

## Procedure to Integrate

Configure **Firewall Analyzer** Settings

1. Connect web client to OpManager server.
2. Open the URL: '**https://<Machine Name/IP Address of the OpManager server>**', in a browser.
3. Login page appears, enter the credentials. OpManager dashboard appears.

To configure the Firewall Analyzer Settings in OpManager

4. Click **Admin** tab.
5. In the **Tools** section, click **Add-On/Products Integration**
6. Click **Firewall Settings** icon in this screen. Type the following Firewall Analyzer server details:
  - a. Server Name
  - b. Port (default is 8500)
  - c. User Name
  - d. Password
  - e. Polling Interval in mins
7. Click **Test Connection and Save** to test the Firewall Analyzer server connection from OpManager server and save the settings.

## Viewing the Firewall Analyzer reports from the OpManager

Only Servers and Firewalls are supported.

After configuring the settings, you can follow the steps given below to see the detailed reports:

For **Servers**

1. Go to the Servers map.
2. Click the required server icon in the Servers map to see its snapshot page.
3. Click the **Reports** combo box.
4. Select one of the reports as required:
  - a. Top Clients
  - b. Top Triggered Rules
  - c. Top URLs

- d. Top Denied Requests
- e. Top Attacks
- f. Top conversations
- g. Top Protocol Groups

#### For **Firewalls**

1. Go to the Servers map.
2. Click the required server icon in the Servers map to see its snapshot page.
3. Click the **Reports** combo box.
4. Select one of the reports as required:
  - a. Traffic Reports
  - b. Security Reports
  - c. All Reports



You will be prompted to log on with the Firewall Analyzer's administrator user name and password the first time you view the report.

## Using Ask ME

---

The **Ask ME** tab offers a quick way to see just the reports that you need, without having to create a new report profile, or drilling down through the pre-defined reports.

Ask ME enables managers and other non-technical staff to answer simple but critical questions about bandwidth usage and network security.

The Ask ME tab shows a series of questions. In Step 1, select the area of interest in the "**I have a question about...**" combo box - bandwidth usage, firewall rules, etc. If you are not sure, leave it to the default *All Questions* option.

In Step 2, select the appropriate Firewall for which you need a report in the "**Reporting for** " combo box. If you are not sure, leave it to the default *All Firewalls* option.

In Step 3, select the appropriate question for which you need an answer. Then click the **Get the Answer** button.

The report corresponding to the question and the Firewall selected is now generated and displayed.

If you want more questions to come up in the Ask ME tab, click the **Tell us here** link. In the popup window that opens, enter the question and describe it shortly. Once you are done, click **Send**.

The Firewall Analyzer Technical Support team will analyze your question, and if found valid, will include it in upcoming releases of Firewall Analyzer.

## Contacting Technical Support

The **Support** tab gives you a wide range of options to contact the Technical Support team in case you run into any problems.

| Link                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Request Technical Support             | Click this link to submit a form from the Firewall Analyzer web site, with a detailed description of the problem that you encountered                                                                                                                                                                                                                                                                      |
| Troubleshooting Tips                  | Click this link to see the common problems typically encountered by users, and ways to solve them                                                                                                                                                                                                                                                                                                          |
| Contact Support                       | Call the toll-free number +1 888 720 9500 to talk to the Firewall Analyzer Technical Support team directly                                                                                                                                                                                                                                                                                                 |
| Create Support Information File [SIF] | Click this link to create a ZIP file containing all the server logs that the Technical Support team will need, to analyze your problem. You can then send this ZIP file to fwanalyzer-support@manageengine.com or upload the ZIP file to our ftp server by clicking on Upload to <b>FTP Server</b> , in the pop-up window provide your E-Mail id and browse for the zipped SIF file and then press Upload. |
| Need a Feature                        | Click this link to submit a feature request from the Firewall Analyzer web site                                                                                                                                                                                                                                                                                                                            |
| User Forums                           | Click this link to go to the Firewall Analyzer user forum. Here you can discuss with other Firewall Analyzer users and understand how Firewall Analyzer is being used across different environments                                                                                                                                                                                                        |
| Feedback                              | At any time, you can click the <b>Feedback</b> link in the top pane, to send any issues or comments to the Firewall Analyzer Technical Support team.                                                                                                                                                                                                                                                       |

The Support tab displays the latest discussions in the Firewall Analyzer User Forum.

### Procedure to resolve Firewall Analyzer issue with Firewall Analyzer support

Best in the industry technical support and other informal means to get Firewall Analyzer issues resolved.

Adopt the following ways progressively.

#### Knowledge Base & Community

- Go through the FAQ
- Look out in the trouble shooting tips
- Browse through the Firewall Analyzer forum

#### Best in the industry technical support

- Send email to fwanalyzer-support@manageengine.com
- Call toll free telephone number (+1-888-720-9500)
- Ask for a meeting (**Zoho Meeting**) – web conference

### **Procedure to create a Support Information File (SIF) and send the SIF to Firewall Analyzer support**

We would recommend the user to create a **Support Information File (SIF)** and send the SIF to [fwanalyzer-support@manageengine.com](mailto:fwanalyzer-support@manageengine.com). The SIF will help us to analyze the issue you have come across and propose a solution.

The instructions for creating the SIF is as follows:

- Login to the Web-client and click the **Support** tab.
- Click the **Create Support Information File** link shown in that page.
- Wait for 30-40 Secs and again click the **Support** tab.
- Now you will find new links **Download** and **Upload to FTPServer**.
- You can either download the SIF by clicking on the **Download** link and then send the downloaded SIF to [fwanalyzer-support@manageengine.com](mailto:fwanalyzer-support@manageengine.com) or click the **Upload to FTPServer** and provide the details asked and upload the file.

### **Procedure to create SIF and send the file to ManageEngine, if the Firewall Analyzer server or web client is not working**

If you are unable to create a SIF from the web client UI, you can zip the files under '*log*' folder, which is located in *<Firewall Analyzer Home>\server\default\log* (default path) and send the zip file by uploading it in the following ftp link:  
<http://bonitas.zohocorp.com/upload/index.jsp?to=fwanalyzer-support@manageengine.com>